21世纪高等学校规划教材 | 信息管理与信息系统



信息安全管理与风险评估

赵　刚　编著

清华大学出版社

21世纪高等学校规划教材·信息管理与信息系统

信息安全管理与风险评估

赵　刚　编著

清华大学出版社
北　京

内 容 简 介

本书在系统归纳国内外信息安全管理与风险评估的最佳实践以及近年来研究成果的基础上，全面介绍了信息安全管理、信息安全管理体系、信息安全风险评估的基本知识、相关标准和各项内容，全书涵盖了信息安全管理体系建立流程、风险评估实施流程，以及信息系统安全等级保护、云计算安全管理与风险评估、IT 治理等内容。

本书既可作为高等院校信息安全专业、信息管理与信息系统专业、管理科学与工程专业及计算机相关专业的本科生和研究生的教材，也可作为从事信息化相关工作的管理人员、信息安全管理人员、网络与信息系统安全管理人员、IT 相关人员的参考书。

图书在版编目(CIP)数据

信息安全管理与风险评估/赵刚编著. --北京：清华大学出版社，2013
21 世纪高等学校规划教材・信息管理与信息系统
ISBN 978-7-302-33600-6

Ⅰ. ①信…　Ⅱ. ①赵…　Ⅲ. ①信息系统－安全管理－高等学校－教材 ②信息系统－安全技术－风险分析－高等学校－教材　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2013)第 203897 号

责任编辑：魏江江　薛　阳
封面设计：
责任校对：时翠兰
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：13.25　　**字　　数**：315 千字
版　　次：2014 年 1 月第 1 版　　**印　　次**：2014 年 1 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：053926-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程”（简称“质量工程”），通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上。精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前，针对计算机类和电子信息类相关专业成立了两个“编委会”，即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括：

(1) 21世纪高等学校规划教材·计算机应用——高等学校各类专业，特别是非计算机专业的计算机应用类教材。

(2) 21世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21世纪高等学校规划教材·信息管理与信息系统。

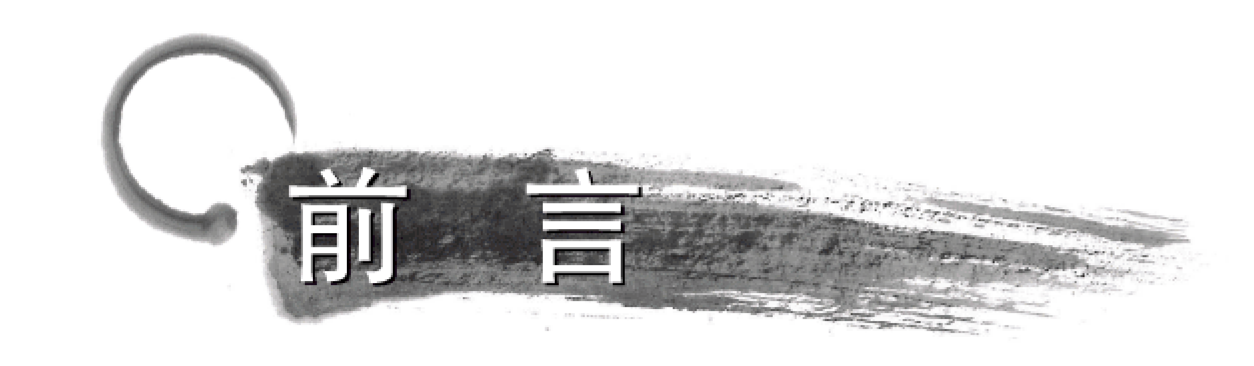
(6) 21世纪高等学校规划教材·财经管理与应用。

(7) 21世纪高等学校规划教材·电子商务。

(8) 21世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力，在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌，为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格，这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会
联系人：魏江江
E-mail：weijj@tup.tsinghua.edu.cn



前　言

信息化已融入到人类社会的每一个角落,不断推动着社会的进步和发展。然而,无处不在的信息孕育着随时可能发生的风险,信息安全事件时有发生,信息安全问题也成为全社会共同关注的问题,信息系统的安全、管理、风险与控制日益成为突出的问题。信息安全研究所涉及的领域相当广泛,信息安全的建设是一个系统工程,正确的做法是遵循国内外相关信息安全标准与最佳实践,考虑组织对信息安全各个层面的需求,在风险评估的基础上引入合理的控制措施,建立信息安全管理体系以保证信息的安全属性。绝大多数信息安全问题是管理方面的缺陷,因此信息安全管理是十分重要的课题,在解决信息安全问题中占重要地位,其发展对信息安全人才的培养提出了更高的要求。风险评估是信息安全管理体系和信息安全风险管理的基础,是建立信息安全保障体系的必要前提,通过风险评估能够将信息安全活动的重点放在重要的问题上。本书旨在通过本课程的学习,帮助学生了解信息安全管理、信息安全风险评估的基本知识、相关标准,理解信息安全管理体系的建立过程以及风险评估的实施过程,进而在实际工作中得到应用,对组织的具体实践提供理论指导,帮助组织建立合理的信息安全管理体系。

本书从信息安全管理、风险评估的概念出发,全面、系统地介绍了信息安全管理体系、信息安全风险评估、信息系统安全等级保护、云计算安全管理与风险评估、IT 治理等内容。全书由基本知识、信息安全风险评估、信息安全管理三部分构成,共分为 11 章。第 1 章引论,着重介绍了信息安全管理和风险评估相关的基本概念及其发展过程、现状和发展趋势,初步介绍了信息安全管理与风险评估的关系;第 2 章信息安全管理的主要内容,主要介绍了信息安全管理体系模型、建立信息安全管理体系的基本过程,讨论了国内外信息安全管理相关标准以及主要的信息安全管理工具;第 3 章信息安全风险评估的主要内容,主要介绍了风险评估模型、实施风险评估的总体流程,讨论了国内外相关标准以及主要的风险评估工具;第 4 章 IT 治理概述,主要介绍了 IT 治理概念和基础内容,围绕国际上公认的 IT 治理标准,重点讨论了 IT 治理支持手段;第 5 章信息安全风险评估实施流程,充分讨论了风险评估准备、资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险分析等实施风险评估的各阶段作业流程和各方面内容,介绍了风险处置计划和风险评估报告的内容;第 6 章信息系统生命周期各阶段的风险评估,介绍了信息系统生命周期中规划阶段、设计阶段、实施阶段、运维阶段和废弃阶段中风险评估的工作内容;第 7 章建立信息安全管理体系的工作流程,深入细致地讨论了信息安全管理体系的策划与准备、设计与建立、实施与运行、体系审核、改进与保持等各阶段的工作内容;第 8 章信息安全管理体系的认证,从信息安全管理体系认证概念出发,介绍了认证的目的、范围、认证机构,及认证过程等内容;第 9 章信息安全管理控制措施,详细阐述了选择控制措施的方法和过程,围绕国内外较为通用的标准,重点讨论了信息安全管理控制规范;第 10 章信息系统安全等级保护标准体系,从等级保护基本知识出发,详细讨论了等级保护实施方法和过程,着重分析了等级保护与信息安全管理体

系、等级保护与信息安全风险评估的关系；第 11 章云计算的安全管理与风险评估，介绍了云计算的模式与架构，着重分析了云计算的信息安全问题，重点讨论了云计算风险评估的特点和方式，深入阐述了云计算的风险控制措施。

全书结构合理、内容全面、概念清晰、深入浅出，符合教学特点和需求，业务实用性强，紧跟信息安全管理与风险评估研究以及 IT 应用的发展趋势，融入了最新的创新内容。

本书既可作为高等院校信息安全专业、信息管理与信息系统专业、管理科学与工程专业及计算机相关专业的本科生和研究生的教材，也可作为从事信息化相关工作的管理人员、信息安全管理人员、网络与信息系统安全管理人员、IT 相关人员的参考书。

本书是作者长期从事理论研究和科学实践以及教学经验和成果的归纳总结，作者精心设计安排全书的结构和内容，以适应不同层次和不同专业读者的需求。书中汲取了大量国内外本领域代表文献的精华，参考了大量的国内外有关研究成果，在此，谨向书中提到和参考文献列出的作者表示感谢。作者所指导的学生刘换、宋健豪等参与了编写本书的相关工作，在此一并表示感谢。同时感谢北京信息科技大学信息管理学院的领导、全体教师的大力支持和帮助。最后，衷心感谢清华大学出版社为本书出版付出的辛勤劳动。

信息技术在飞速发展，信息安全管理和风险评估也在不断创新和发展，其理念和技术等都在不断地更新。书稿虽经多次修改，但由于作者水平有限，书中难免存在不足和疏漏之处，诚望使用本教材的师生和读者不吝指教。

本书配套的教学电子课件，读者可登录清华大学出版社网站（http://www.tup.com.cn）下载。

编　者

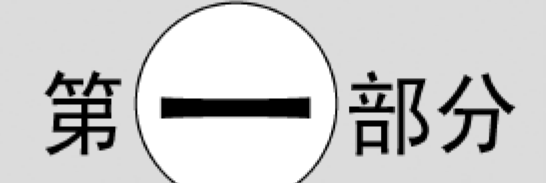
2013 年 4 月于北京



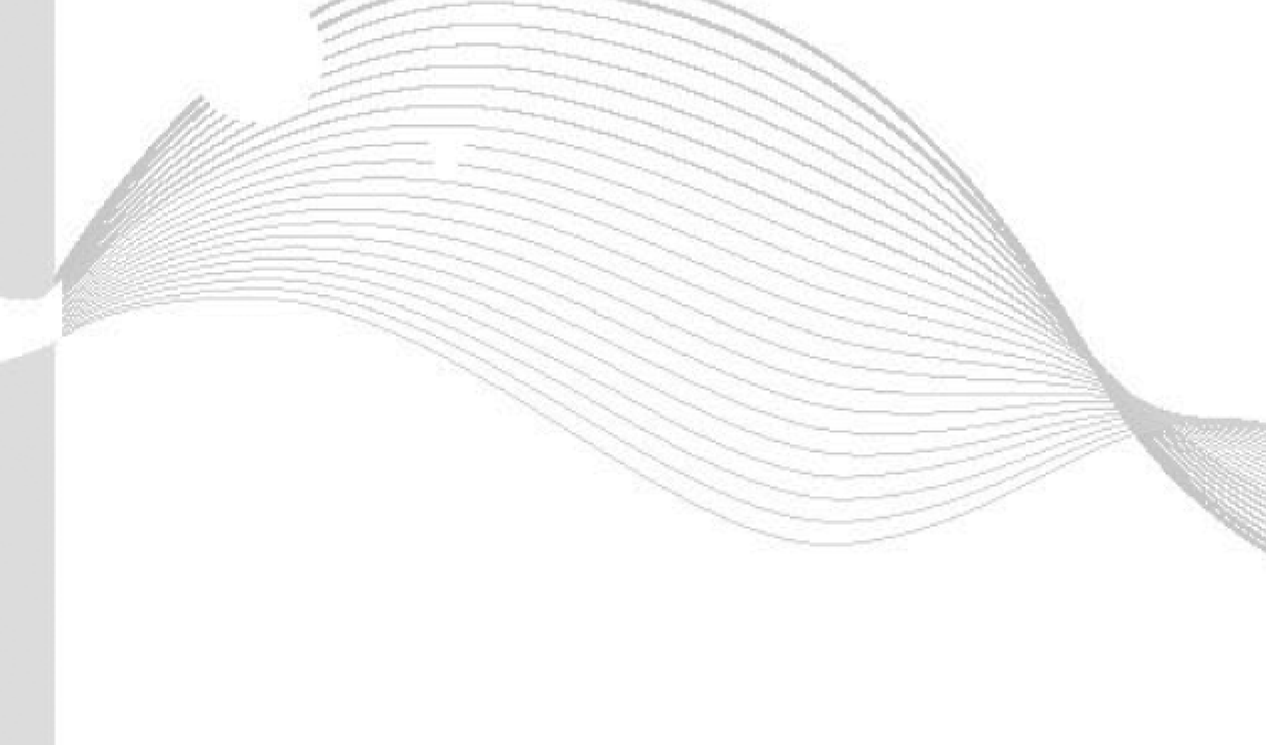
第一部分　基 本 知 识

第二部分 信息安全风险评估

第三部分 信息安全管理



基本知识



第1章 引论

1.1 信息安全管理概述

人类社会已经进入了信息时代，当今社会的发展对信息资源依赖的程度越来越大，从人们日常生活、组织运作，到国家管理，信息资源都已成为不可或缺的重要资源，信息已经渗透到了人类社会的每一个角落，融入了人们生活的每一个细节，没有各种信息的支持，现代社会将不能继续生存和发展下去。信息已经成为人类的重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用。然而，信息在成为人类重要资产、为人们所用、给人们带来巨大价值的同时，也受到了各种各样来自于组织内部与外部威胁的冲击，信息安全事件在全球范围内屡屡发生，由于计算机技术的迅猛发展而带来的信息安全问题正变得日益突出，给人类社会的发展带来了巨大损失。

信息安全管理是随着信息和信息安全的发展而发展的。由于信息具有易传播、易扩散、易损毁的特点，信息资产比传统的实物资产更加脆弱，更容易受到损害，这样将使组织在业务运作过程中面临巨大的风险。这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞，以及大量存在于组织内外的各种威胁。因此，对信息系统需要加以严格管理和妥善保护，信息安全管理也随之产生。

1.1.1 信息安全管理的内涵

1. 信息

信息(Information)的定义多种多样。国际公认的 ISO/IEC 信息技术安全管理指南(GMITS)对信息给出如下解释：信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。信息可以简单地定义为经过加工的数据或消息，是对决策者有价值的数据。一般意义上的信息是指事物运动的状态和方式，是事物的一种属性，在引入必要的约束条件后可以形成特定的概念体系。通常情况下，可以把信息理解为消息、信号、数据、情报、知识，可以是信息设施中存储与处理的数据、程序，可以是打印或书写出来的论文、电子邮件、设计图纸、业务方案，也可以是显示在胶片等载体或表达在会话中的消息。

2. 信息系统的定义

GB 17859—1999《计算机信息系统安全保护等级划分准则》定义：计算机信息系统是由

计算机及其相关的和配套的设备、设施(含网络)构成的,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。毫无疑问,计算机及各类通信网络的出现与蓬勃发展使信息技术出现了前所未有的革命,也使信息量急剧膨胀。

3. 信息安全的定义

信息安全是一个广泛而抽象的概念,不同领域的不同方面对其概念的阐述都会有所不同,建立在网络基础之上的现代信息系统,其安全定义较为明确,其定义为:保护信息系统的硬件、软件及相关数据,使之不因为偶然或恶意侵犯而遭到破坏、更改及泄漏,保证信息系统能够连续、可靠、正常地运行。在商业和经济领域,资产是任何对组织有价值的事物,像其他重要的业务资产一样,信息是一种资产。对于一个组织的业务,信息资产是其中的关键,随着业务互联的增加,造成信息暴露出更多数量、更广范围的威胁和脆弱性,需要得到适当的保护。因此,信息安全主要强调的是保障信息不受威胁的侵扰,消减并控制风险,保持业务操作的连续性,将风险造成的损失和影响降到最低,并且获得最大化的投资回报和商业机会。

信息安全通过实施一套控制措施,包括方针、过程、程序、组织结构和软件硬件功能来实现。这些控制措施需要建立、实施、评审以及改进,以保障组织特定的安全和业务目标。

在信息保障的概念中,信息安全一般包括实体安全、运行安全、信息安全和管理安全4个方面的内容。实体安全包括环境安全、设备安全、媒体安全3个方面。运行安全包括风险分析、审计跟踪、备份和恢复、应急4个方面。信息安全包括操作系统安全、数据库安全、网络安全、病毒保护、访问控制、加密与鉴别7个方面。管理安全是指通过信息安全相关的法令和规章制度以及安全管理手段,确保信息安全生存与运营。

4. 信息安全属性

从信息安全属性出发,将信息安全的主要目标定义为信息的机密性、完整性和可用性的保持。ISO/IEC 13335-1:2004以及ISO/IEC 27002:2005中将信息安全定义为:保护信息的保密性(Confidentiality)、完整性(Integrity)、可用性(Availability)及其他属性,包括真实性(Authenticity)、可审核性(Accountability)、不可否认性(non-repudiation)和可靠性(Reliability)等。可用性是指已授权实体一旦需要就可访问和使用的特性;保密性是指使信息不泄漏给未授权的个人、实体、过程或不使信息为其利用的特性;完整性是指数据未经授权不可修改或破坏的特性,如图1-1所示。

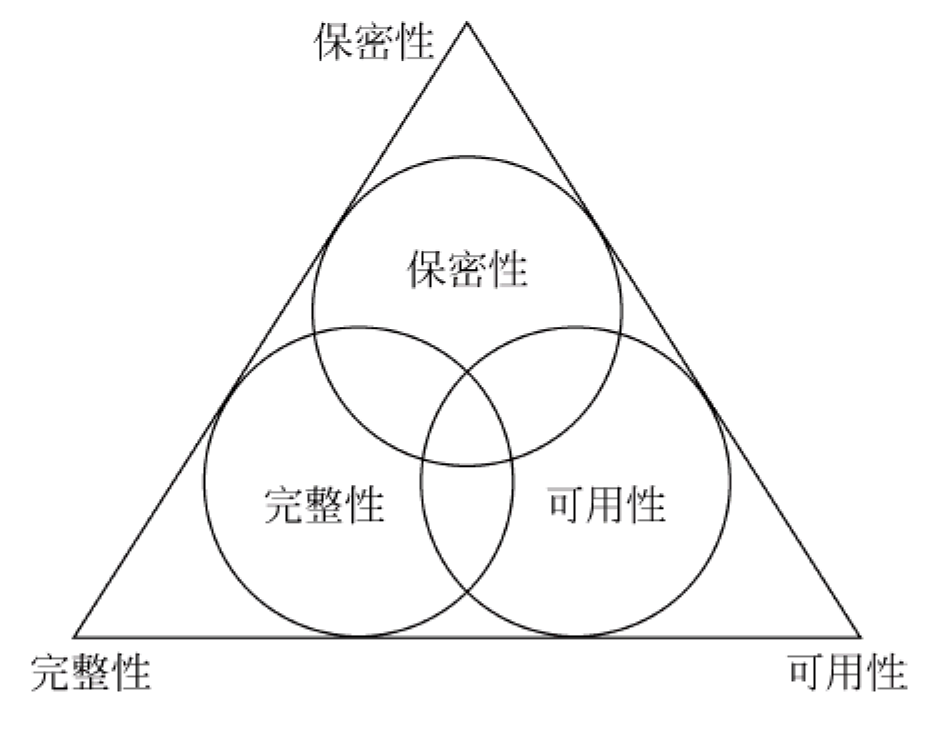


图1-1 安全属性

5. 信息安全管理及其内容

信息安全管理是通过维护信息的机密性、完整性和可用性等来管理和保护信息资产的一项体制,是对信息安全保障进行指导、规范和管理的一系列活动和过程。管理体系包括组织机构、策略、策划、活动、职责、惯例、程序、过程和资源。

6. 信息安全管理体系

信息安全管理体系(Information Security

Management System，ISMS）是组织在整体或特定范围内建立的信息安全方针和目标，以及完成这些目标所用的方法和手段所构成的体系。信息安全管理体系属于整体管理体系的一部分，是信息安全管理活动的直接结果，表示为方针、原则、目标、方法、计划、活动、程序、过程和资源的集合。

信息安全管理体系是一个系统化、程序化和文件化的管理体系，具有以下特点。

（1）体系的建立基于系统、全面、科学的安全风险评估，体现以预防控制为主的思想。

（2）强调遵守国家有关信息安全的法律、法规及其他合同方要求。

（3）强调全过程和动态控制，本着控制费用与风险平衡的原则，合理选择安全控制方式。

（4）强调保护组织所拥有的关键性信息资产，而不是全部信息资产，确保信息的机密性、完整性和可用性，保持组织的竞争优势和业务运作的持续性。

建立信息安全管理体系通常起到以下作用：

（1）强化员工的信息安全意识，规范组织信息安全行为。

（2）组织管理层贯彻信息安全保障体系。

（3）对组织制定具体工作计划的关键信息资产进行全面系统的保护，维持竞争优势。

（4）在信息系统受到侵袭时，确保业务持续开展并将损失降到可接受的水平。

（5）使组织的生意伙伴和客户对组织充满信心。

（6）如果通过系统认证，表明体系符合标准，证明组织有能力保障重要信息，可以提高组织的知名度与信任度。

（7）组织可以参照信息安全管理模型，按照先进的信息安全管理标准、建立组织完整的信息安全管理体系并实施与保持，达到动态的、系统的、全员参与、制度化的、以预防为主的信息安全管理方式，用最低的成本，达到可接受的信息安全水平，从根本上保证业务的连续性。

1.1.2　信息安全管理发展状况

1. 国外信息安全管理现状

国际上信息安全管理近几年的发展主要包括以下几个方面。

1）制定信息安全发展战略和计划

制定发展战略和计划是发达国家一贯的作法。美、俄、日等国家都已经或正在制定自己的信息安全发展战略和发展计划，确保信息安全沿着正确的方向发展。2000 年年初，美国出台了计算机空间安全计划，旨在加强关键基础设施、计算机系统和网络免受威胁的防御能力。2000 年 7 月，日本信息技术战略本部及信息安全会议拟定了信息安全指导方针。2000 年 9 月 12 日，俄罗斯批准了《国家信息安全构想》，明确了保护信息安全的措施。

2）加强信息安全立法，实现统一和规范管理

以法律的形式规定和规范信息安全工作是有效实施安全措施的最有力保证。制定网络信息安全规则的先锋是各大门户网站，一些大型美国网站都在实践中形成了一套自己的信息安全管理办法。2000 年 10 月 1 日，美国的电子签名法案正式生效。2000 年 10 月 5 日美参议院通过了《互联网网络完备性及关键设备保护法案》。日本邮政省于 2000 年 6 月 8 日

公布了旨在对付黑客的《信息网络安全可靠性基准》的补充修改方案，提出并制定了有关风险管理的“信息安全准则”指导原则。2000年9月，俄罗斯实施了关于网络信息安全的法律。

3）步入标准化与系统化管理时代

在20世纪90年代之前，信息安全主要依靠安全技术手段与不成体系的管理规章来实现。随着20世纪80年代ISO 9000质量管理标准的出现及随后在全世界的推广应用，系统管理的思想在其他管理领域也被借鉴与采用，如后来的ISO 14000环境体系管理标准、OHSAS 18000职业安全卫生管理体系标准，信息安全管理也同样在20世纪90年代步入了标准化与系统化管理的时代。

1995年，英国率先推出了BS 7799信息安全管理标准，该标准于2000年被国际标准化组织认可为国际标准ISO/IEC 17799。现在该标准已引起许多国家与地区的重视，在一些国家已经被推广与应用。

2. 国内信息安全管理现状

在威胁多样化的信息化时代，我国信息安全管理的现状不容乐观，这可以从国家宏观管理与组织微观管理两方面来加以论述。

在国家宏观信息安全管理方面，主要有以下问题。

1）法律法规问题

健全的信息安全法律法规体系是确保国家信息安全的基础，是信息安全的第一道防线。我国已建立了法律、行政法规与部门规章、规范性文件这三个层面的有关信息安全的法律法规体系，对组织与个人的信息安全行为提出了安全要求。但是，我国的法律法规体系还存在缺陷，一是现有的法律法规存在不完善的地方，如法律法规之间有内容重复交叉，同一行为有多个行政处罚主体，有的规章与行政法规相互抵触，处罚幅度不一致；二是法律法规建设跟不上信息技术发展的需要，这主要涉及网络规划与建设、网络管理与经营、网络安全、数据的法律保护、电子资金划转的法律认证、计算机犯罪与刑事立法、计算机证据的法律效力等方面的法律法规缺乏或有待完善。

2）管理问题

管理包括三个层次的内容：组织建设、制度建设和人员意识。组织建设是指有关信息安全管理机构的建设。信息安全的管理包括安全规划、风险管理、应急计划、安全教育培训、安全系统的评估、安全认证等多方面的内容，因此只靠一个机构是无法解决这些问题的。在各信息安全管理机构之间，要有明确的分工，以避免“政出多门”和“政策拉车”现象的发生。明确了各机构的职责之后，还需要建立切实可行的规章制度，即进行制度建设，以保证信息安全。如对人的管理，需要解决多人负责、责任到人的问题，任期有限的问题，职责分离的问题，最小权限的问题等。有了组织机构和相应的制度，还需要领导的高度重视和群防群治，即强化人员的安全意识，这需要信息安全意识的教育和培训，以及对信息安全问题的高度重视。

3）国家信息基础设施建设问题

关于国家信息基础设施方面存在的问题已引起国家的高度重视。《国家信息安全报告》指出：我国计算机硬件、通信设备制造业的基础集成电路芯片，主要依赖进口，系统软件、支

撑软件基本上是国外产品。在这种形势下,我们必须清醒地承认一个基本事实:构成我国信息基础设施的网络、硬件、软件等产品几乎完全是建立在外国的核心信息技术之上的。

我国在微观信息安全管理方面存在的问题主要表现为以下几点。

1)缺乏信息安全意识与明确的信息安全方针

大多数组织的最高管理层对信息资产所面临威胁的严重性认识不足,或者仅局限于IT方面的安全,没有形成一个合理的信息安全方针来指导组织的信息安全管理工作,这表现为缺乏完整的信息安全管理制度,缺乏对员工进行必要的安全法律法规和防范安全风险的教育与培训,组织未必能严格实施现有的安全规章等。

2)重视安全技术,轻视安全管理

目前组织广泛采用现代通信、计算机和网络技术来构建信息系统,以提高组织效率与竞争能力,但相应的管理措施不到位,如系统的运行、维护和开发等岗位不清,职责不分,存在一人身兼数职现象。而大约70%以上的信息安全问题是由管理方面的原因造成的,也就是说,解决信息安全问题不仅应从技术方面着手,同时更应加强信息安全的管理工作。

3)安全管理缺乏系统管理的思想

大多数组织现有的安全管理模式仍是传统的管理方法,出现了问题才去想补救的办法,是一种就事论事、静态的管理,不是建立在信息安全风险评估基础上的、动态的、持续改进的管理方法。

1.2 信息安全风险评估概述

1.2.1 信息安全风险评估的内涵

1. 基本概念

信息安全风险评估是从风险管理角度,运用定性、定量的科学分析方法和手段,系统地分析信息和信息系统等资产所面临的、人为的和自然的威胁,以及威胁事件一旦发生可能遭受的危害程度,有针对性地提出抵御威胁的安全等级防护对策和整改措施,从而最大限度地减少经济损失和负面影响。

风险评估(Risk Assessment)是对信息和信息处理设施的威胁、影响和薄弱点及三者发生的可能性的评估。风险评估也是确认安全风险及其大小的过程,即利用适当的风险评估工具,包括定性和定量的方法,确定资产风险等级和优先控制顺序。

2. 风险评估特征

目前的风险评估具有如下的基本特征:

(1)风险评估包括信息系统安全的众多方面,如资产、人员、管理体系、物理、主机、网络分析等。漏洞扫描、防范与攻击,以及入侵检测等安全技术作为风险评估的手段,为评估提供了必要的分析数据。

(2)系统风险评估不仅是一个具体的产品、工具,更是一个过程、一个体系。完善的系统风险评估体系应包括相应的组织架构、业务、标准和技术体系。

（3）评估过程的主观性是影响评估结果的一个相当重要而又是最难解决的方面。在系统风险评估中，主观性是不可避免的，我们所要做的是尽量减少人为主观性，目前在该领域利用神经网络、专家系统、决策树等人工智能技术进行的研究比较活跃。

（4）风险评估工具比较缺乏，市场上关于漏洞扫描、防火墙等都有比较成熟的产品，但与系统风险评估相关、有效的工具还比较匮乏。

“没有规矩，不成方圆”，这句话在信息系统风险评估领域也是适用的，没有标准指导下的风险评估是没有任何意义的。通过依据某个标准的风险评估或者得到该标准的评估认证，不但可为信息系统提供可靠的安全服务，而且可以树立单位良好的信息安全形象。

1.2.2 风险评估的意义

毫无疑问，风险评估是了解信息系统安全风险的重要手段。风险评估的最终目的是指导信息系统的安全建设，安全建设的实质是控制信息安全风险。风险评估结果是后续安全建设的依据。单独的信息系统的安全风险值没有实际意义，不能将计算风险值作为风险评估的唯一重点，也不能把风险值作为风险评估的唯一成果。如果将风险评估视为对风险值的数据处理，那么这是一种误区。

信息安全工程过程中，首要一步是分析安全需求，这要通过风险评估来完成，风险评估工作对信息安全保障建设的重要意义便在于此。因此，必须重视风险评估每一步骤的结果，在很多情况下，这些结果比最后的风险值更有意义。

风险的控制措施有 4 种，分别为接受风险、降低风险、规避风险和转移风险，这与风险值和成本因素密切相关。

一般情况下，采取安全措施的成本要小于信息安全事件的后果。因此，安全措施的选择需要利用威胁评估与脆弱性评估的结果。可将风险控制的实质描述为：

（1）当存在系统脆弱性时，修补系统脆弱性，降低脆弱性被攻击的可能性。

（2）当系统脆弱性可被恶意攻击利用时，运用层次化保护、结构化设计、管理控制等办法将风险最小化或防止脆弱性被利用。

（3）当攻击者的成本小于攻击的可能所得时，运用保护措施，通过提高攻击者成本来降低攻击者的攻击动机，例如限制系统用户的访问对象和行为。

（4）当损失巨大时，运用系统设计中的基本原则及结构化设计、技术或非技术类保护措施来限制攻击的范围，从而降低可能的损失。

1.2.3 信息安全风险评估发展状况

1. 国外信息安全风险评估发展概况

1）美国信息安全风险评估发展概况

在国际上，美国是对信息安全风险评估研究历史最长和经验最丰富的国家，一直主导信息技术和信息安全的发展，信息安全风险评估在美国的发展实际上也代表了风险评估的国际发展趋势。从最初关注计算机保密发展到目前关注信息系统基础设施的信息保障，大体经历了三个阶段，见表 1-1。

表 1-1 风险评估发展过程

性质＼阶段	第一阶段 以计算机为对象的保密阶段	第二阶段 以网络为对象的保护阶段	第三阶段 以信息基础设施为对象的保障阶段
时间	20 世纪 60 年代至 20 世纪 70 年代	20 世纪 80 年代至 20 世纪 90 年代	20 世纪 90 年代末至今
评估对象	计算机	计算机和网络	信息系统关键基础设施
背景	计算机开始应用于政府军队	计算机系统形成了网络化的应用	计算机网络系统成为关键基础设施的核心
标志性事件	事件 1～事件 3	事件 4～事件 8	事件 9～事件 14
特点	对安全的评估仅限于保密性	逐步认识到了更多的信息安全属性(保密性、完整性、可用性)	安全属性扩大到了保密性、完整性、可用性、可控性、不可否认性等多个方面

标志性事件如下。

事件 1：1967 年 11 月，美国国防科学委员会委托兰德公司、迈特公司及其他和国防工业有关的一些公司，开始研究计算机安全问题。到 1970 年 2 月，经过将近两年半的工作，主要对当时的大型计算机、远程终端进行了研究分析，作了第一次规模比较大的风险评估。1970 年年初，形成了一份长达数百页的机密报告《计算机安全控制》，该报告奠定了国际安全风险评估的理论基础。

事件 2：1974 年，美国推出了 FIPS PUB31 自动数据处理系统物理安全和风险管理指南，是首批推出的关于信息安全风险管理及安全测评的标准。

事件 3：1979 年，美国推出了 FIPS PUB65 自动数据处理系统风险分析指南。

事件 4：出现了初期的针对美国军方的计算机黑客行为，1988—1989 年，美国的计算机网络出现了一系列重大事件，美国的审计总署(GAO)对美国主要由国防部使用的计算机网络进行了大规模的持续评估。

事件 5：1990 年，美国建立了信息安全事件响应国际论坛(FIRST)。

事件 6：1992 年，美国国防部建立了漏洞分析与评估计划。

事件 7：1993 年，美国和欧洲 4 国(英、法、德、荷)、加拿大以及国际标准化组织(ISO)开始共同制定了信息技术安全通用评估准则(CC)。1999 年成为国际标准 ISO/IEC 15408。

事件 8：1995 年 9 月至 1996 年 4 月，美国的审计总署为响应国会“加强信息安全，降低信息战威胁”的要求，对美国国防系统的信息系统进行了大规模风险评估，1996 年 5 月发表了报告《信息安全——针对国防部的计算机攻击正构成日益增大的风险》。

事件 9：1997 年 12 月，美国国防部发布了《国防部 IT 安全认证和认可过程》(DITSCAP)，成为美国涉密信息系统的安全评估和风险管理的重要标准和依据。

事件 10：2000 年 4 月，负责国家安全系统的国家安全系统委员会发布了专门针对国家安全系统的《国家信息保障认证和认可过程》(NIACAP)。

事件 11：美国国家标准与技术局(NIST)在 2000 年 11 月制定的《联邦 IT 安全评估框架》中提出了自评估的 5 个级别。针对该框架，NIST 颁布了《IT 系统安全自评估指南》(SP 800-26)，为三大类 17 项安全控制提出了 17 张调查表。

事件 12：2002 年 1 月，NIST 发布了《IT 系统风险管理指南》(SP 800-30)，概述了风险评估的重要性、风险评估在系统生命周期中的地位、进行风险评估的角色和任务；阐明了风

险评估的步骤、风险缓解的控制和评估评价的方法。

事件 13：2002 年颁布了《联邦信息安全管理法案》(FISMA)，提出联邦各机构的信息安全项目必须包括定期的风险评估、基于风险评估的政策和流程、安全计划、安全意识培训计划、对安全的定期测试和评估、对安全事件进行检测和响应的流程以及用来确保信息系统运行连续性的计划和流程。

事件 14：从 2002 年 10 月开始，NIST 先后发布了《联邦 IT 系统安全认证和认可指南》(SP 800-37)、《联邦信息和信息系统的安全分类标准》(FIPS 199)、《联邦 IT 系统最小安全控制》(SP 800-53)、《将各种信息和信息系统映射到安全类别的指南》(SP 800-60)等多个文档，试图以风险思想为基础加强联邦政府的信息安全。

2) 其他国家信息安全评估发展概况

欧洲在信息化方面的优势不如美国，但作为多个老牌大国的联合群体，欧洲不甘落后。它们在信息安全管理方面的作法是在充分利用美国引导的科技创新成果的基础上，加强预防。欧洲诸国在风险管理上一直探索走一条不同于美国的道路。“趋利避害”一直是欧洲各国在信息化进程中防范安全风险的共同策略。信息安全风险管理和评估研究工作一直是欧盟投入的重点。

亚洲各国多为信息化领域的发展中国家，它们大多采取抢抓信息化发展机遇，把发展放在首位的战略，风险管理工作均是为了更好的发展，比如日本在风险管理方面就综合了美国和英国的作法，建立了“安全管理系统评估制度”，作为日本标准(JIS)，启用了 ISO/IEC 17799-1(BS 7799)指导政府和民间的风险管理实践。韩国主要参照美国的政策和方法，通过专门成立的信息安全局，强力推进风险管理的实践。新加坡主要参照英国的作法，在信息安全风险评估方面依据 BS 7799，并向亚洲邻国输出其信息安全风险管理的专门知识和服务。

重大事件如下。

事件 1：1995 年，澳大利亚/新西兰风险管理准则联合委员会颁布了世界上第一部风险管理的正式标准——AS/NZS 4360。这是一个针对普遍风险(而非信息安全风险)的风险管理标准，成为关注一般风险管理人员的通用准则。

事件 2：1995 年，英国标准化协会(BSI)颁布了《信息安全管理指南》(BS 7799)，BS 7799 分为两个部分：BS 7799-1《信息安全管理实施规则》和 BS 7799-2《信息安全管理体系规范》。

事件 3：1996 年，国际标准化组织制定了《信息技术　信息安全管理指南》(ISO/IEC TR 13335)，分成《信息安全的概念和模型》、《信息安全管理和规划》、《信息安全管理技术》、《基线方法》、《网络安全管理指南》5 个部分。

事件 4：1997 年，加拿大风险管理准则委员会颁布了《风险管理：决策者的指导》(AN/CSAQ 850—1997)。

事件 5：1999 年，国际标准化组织发布了《信息技术安全评估共同准则》(CC 标准，ISO/IEC 15408)。

事件 6：2000 年，国际标准化组织通过了依据 BS 7799-1 制定的《信息安全管理实施指南》(ISO/IEC 17779：2000)，提出了基于风险管理的信息安全管理体系。

事件 7：2001 年，德国的联邦信息技术安全局颁布《信息技术基线保护手册》(IT

Baseline Protection Manual (ITBPM or BPM))。BPM 比英国的 BS 7799 更加详细地对威胁和安全措施进行了分类，具体地列出威胁清单和安全措施清单，并通过维护网上更新来实现与时俱进的安全需求。

事件 8：2002 年，英国标准化协会(BSI)颁布了《信息安全管理系统规范说明》(BS 7799-2：2002)。它将信息安全管理的有关问题划分成了 10 个控制要项、36 个控制目标和 127 个控制措施。在 BS 7799-2 中，提出了如何建立信息安全管理体系的步骤。

2. 我国信息安全风险评估发展现状

我国的信息安全风险评估工作是随着对信息安全问题认识的逐步深化不断发展的。早期的信息安全工作中心是信息保密，通过保密检查来发现问题，改进提高。20 世纪 80 年代后，随着计算机的推广应用，随即提出了计算机安全的问题，开展了计算机安全检查工作。

进入 20 世纪 90 年代，随着互联网在我国得到了广泛的社会化应用，国际大环境的信息安全问题和信息战的威胁直接在我国的信息环境中有所反映。1994 年 2 月颁布的《中华人民共和国计算机信息系统安全保护条例》提出了计算机信息系统实行安全等级保护的要求。其后，在有关部门的组织下，不断开展了有关等级保护评价准则、安全产品的测评认证、系统安全等级划分指南的研究，初步提出了一系列相关技术标准和管理规范。信息安全风险意识也开始建立，并逐步有所加强。

近年来，各有关部门及社会各方面积极探索，审慎实践，我国信息安全风险评估开始起步，在信息安全保障工作中发挥了一定的作用，但总体上我国信息安全风险评估工作还处于初始阶段，也存在着一些亟待解决的问题，主要包括：

1) 风险评估角色和责任需要明确

风险评估是责任性极强的严肃工作，因此，在评估中应该有什么人参加，他们应该扮演什么角色，承担什么责任，这些责任通过什么过程和手续体现等问题是需要明确的。否则将对风险评估的实施带来一系列的问题。如评估结果有时缺乏严肃的认可，改进工作的建议和结论时遭束之高阁，很多单位的风险评估工作没有与信息系统生命周期各阶段的安全建设联系起来，仅仅是为了评估而评估，导致风险评估起不到应有的作用。

2) 风险评估实施存在一定风险

由于各单位信息安全保障的现状和问题是涉及单位要害、利益、声誉的事项，所以风险评估是敏感的工作，因此评估本身的安全问题也是非常重要的。目前的风险评估在实施中存在一些问题，如某被评估单位在进行风险评估前，虽然也存在网络入侵现象，但是这些入侵仅处于边缘的试探和扫描，在请外部单位进行评估检测之后，入侵反而直奔系统要害而来；对于实时系统，渗透性测试常有可能导致系统运转失常，影响其可用性；有的评估人员，在离职赴国外学习中，将被评单位的问题和解决办法作为自己的学业论文内容公之于世；另外，目前对系统进行评估测试的工具缺乏统一规范，往往采用国外的工具，这都会对风险评估引入新的风险。

3) 风险评估研究积累不足

信息安全风险评估既是一个管理问题，也是一个技术问题。科学的风险评估需要理论、方法、技术和工具来支撑。我国的科学研究计划中，有关信息安全风险评估的重点科研项目

比较少，对国际上的理论和技术发展的了解、跟踪、分析也不够系统、深入和广泛，目前还未形成国家信息安全风险评估的理论体系架构。此外，也缺乏对不同行业部门的个性化风险的深化研究。随着信息化应用的日益拓展，风险已经更进一步与各个行业的应用、服务、生产的特性密切相关。因此，仅靠目前的IT企业，通用技术平台的脆弱性分析，难以真正掌握和了解具体行业、部门的资产、威胁和风险，也将带来关注面的缺失的问题。

4）风险评估专业技术和管理人才匮乏

熟悉和有能力进行系统安全建设和进行风险评估的专业技术和管理人才匮乏。一些已开始进行信息安全风险评估的国内企业，也是骨干成员边学习、边培养一般业务人员、边进行评估项目，被评单位更是缺乏有能力进行配合的人员。有的人员只是能够对一些设备进行基础的数据测评，缺乏基于多方数据之上的、系统的综合分析与评估的能力。

针对这些信息安全问题，国家采取了具体的应对措施。2003年9月，中共中央办公厅、国务院办公厅转发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号），文件在分析了我国当前信息安全保障工作基本状况的基础上，为进一步提高信息安全保障工作的能力和水平，维护公众利益和国家安全，促进信息化建设健康发展，要求"要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理"。根据27号文件的要求，针对国家重要信息系统和基础信息网络的安全保障需求，为部署和组织各系统和部门的自评估工作，以及为加强信息安全主管部门对重要信息系统和基础信息网络的风险评估工作的监督、检查和指导工作，将采取以下具体措施：

1）建立健全国家重要信息系统和基础信息网络风险评估工作制度

信息安全风险评估作为信息安全保障工作的基础性工作和重要环节，应贯穿于信息系统生命周期的各个阶段。在信息系统的设计、验收及运行维护阶段均应当进行风险评估工作。在信息系统规划设计阶段，应通过风险评估明确系统建设的安全需求和安全目标；在信息系统验收阶段，应通过风险评估验证信息系统安全措施能否实现安全目标；在信息系统运行维护阶段，应定期进行风险评估工作，以检验安全措施的有效性并确保安全目标的实现。当安全形势发生重大变化或信息系统使命有重大变更时，则应及时进行风险评估或再评估。信息系统所有、运营或使用单位应将开展信息安全风险评估工作制度化，定期组织实施信息系统自评估，并积极配合有关部门的检查评估。国家有关职能部门要将督促开展风险评估作为提高信息安全管理水平的重要方法和措施，将开展风险评估工作的情况作为监督检查的重要内容。

2）加强自主评估，落实信息安全等级保护制度

在国家有关部门的督导和国家相关标准的指导下，各单位经常性的自评估和国家主管部门组织的检查评估是风险评估的主要形式，也是实现信息安全等级保护制度的重要措施之一。一方面，各部门和各单位在所管辖的范围内，根据自身的实际情况，明确等级保护的要求，层层落实责任，进行自评估；另一方面，信息安全主管部门依据国家的法律法规和标准规范，将安全检查、机密检查和信息安全工作结合起来，对重要信息系统和基础信息网络进行定期或不定期的检查，评估其等级化建设的落实情况，从而更好地落实国家信息安全等级保护制度。

3）严密组织风险评估工作，遵照科学规范的评估流程

在信息安全风险评估工作开展中应按照“严密组织、规范操作、讲求科学、注重实效”的原则进行。充分认识开展风险评估工作的意义，加强对风险评估工作的组织领导，完善相应的评估机制，保证风险评估工作的科学性、规范性和客观性，形成预防为主、持续改进的风险评估工作制度。同时，风险评估应遵循科学合理的流程，包括资产识别和赋值、威胁和薄弱环节分析、控制措施分析、影响分析、风险计算以及评估总结等关键步骤。避免在评估过程中出现职责不清、有章不循、流于形式、主观臆断等问题。

4）建立健全风险评估信息共享制度，自主研发关键技术和基础环境

在国家重要信息系统建设中，凡涉及互联互通和信息共享的系统都要逐步建立风险评估通报和会商制度。在风险评估中，凡与互联的其他参与者有关的情况，应该依据牵涉范围，及时交换或公布，以便有关联的单位尽早采取应对措施。信息共享的同时，意味着必要的保密责任与义务的转移，因此，既要强调信息共享，也要有制度性的要求，明确共享信息机密、完整、可用的责任和义务。

按照国家信息化发展的需求，逐步完善我国信息安全风险评估相关的标准规范建设，实现管理法制化和规范化。在标准体系建设中，坚持核心技术和关键方法上保持独立自主，又在总体上与国际标准保持衔接。加强风险评估核心技术研究与攻关，提高风险评估的技术水平，并力争在近几年内在核心技术上有较大的突破，为重要信息系统和基础信息网络实施风险评估提供自主可控的工具、模型与实用技术。构建国家基础信息网络风险评估试验环境，满足国家重要信息系统和基础信息网络风险评估的需求，建立国家基础信息网络等关键信息基础设施的风险评估数据库，积累资料。

1.3 信息安全管理与风险评估的关系

信息安全风险评估是信息安全风险管理的一个阶段。信息安全风险管理要依靠风险评估的结果来确定随后的风险控制和审核批准活动。风险评估使得组织能够准确定位风险管理的策略、实践和工具，能够将信息安全活动的重点放在重要的问题上，能够选择成本效益合理的和适用的安全对策。基于风险评估的风险管理方法被实践证明是有效的和实用的，已被广泛应用于各个领域。因此，风险评估是信息安全管理体系和信息安全风险管理的基础，是对现有网络的安全性进行分析的第一手资料，也是网络安全领域内最重要的内容之一，它为实施风险管理和风险控制提供了直接的依据。

了解组织信息安全需求的最主要的方式就是实施风险评估，对信息资产评估风险以后，组织能够：

（1）评审风险的后果，如对组织的业务有什么样的影响与损害。

（2）对怎样管理风险做出决策，比如：接受风险、规避风险、转移风险、降低风险。

（3）采取相应的措施来实施风险管理决策，包括从 ISO/IEC 27001 中选择相关控制目标和控制措施。

在确定风险、管理风险、选择控制目标与控制措施降低风险的过程中，组织应当在业务上考虑各种经济的、业务的、法律的约束条件。风险评估和风险管理是 ISO/IEC 27000 系列中最佳实践和认证过程的重要组成部分。风险管理与风险评估的过程是确定组织安全需

求的重要一环。

思考题

1. 解释“信息安全”、“信息安全管理”的基本概念。
2. 解释“风险评估”的基本概念。
3. 简要叙述“信息安全管理体系”的主要内容。
4. 从技术和管理两方面论述你对信息安全的认识。
5. 查阅资料,论述我国信息安全管理的现状。
6. 查阅资料,论述我国信息安全风险评估的现状。

第2章 信息安全管理的主要内容

2.1 信息安全管理体系模型

2.1.1 信息安全管理体系及其产业链

管理体系是组织用来保证其完成任务，实现目标的过程集的框架。ISO 9000：2000将管理体系定义为建立方针和目标并实现这些目标的体系。

一个组织的管理体系可包括若干不同的管理体系，如质量管理体系、财务管理体系、环境管理体系等。一个典型的管理体系如图2-1所示。

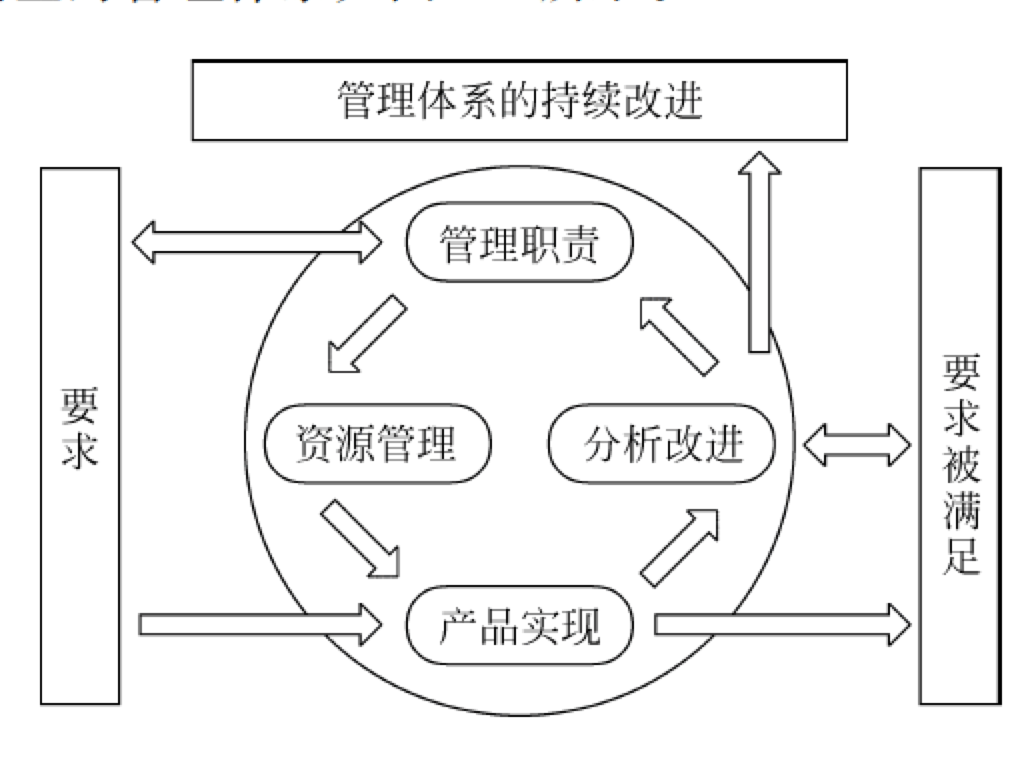


图2-1 管理体系

目前存在很多的管理体系，例如质量管理体系、环境管理体系、职业健康管理体系、信息安全管理体系等。质量管理体系是出现比较早、发展比较成熟的管理体系，其他管理体系或多或少地借鉴了质量管理体系的经验。

管理体系已经形成完整的产业链，如图2-2所示。

信息安全管理体系(Information Security Management System，ISMS)正如其名称所表述的含义，就是关于信息安全的管理体系。ISO/IEC 27001：2005中定义为：信息安全管理体系是整个管理体系的一部分。

ISMS的概念已经跳出了传统的"为了安全信息而信息安全"的理解，它强调的是基于业务风险方法来组织信息安全活动，其本身只是整个管理体系的一部分。这就要求我们站在全局的观点看待信息安全问题。

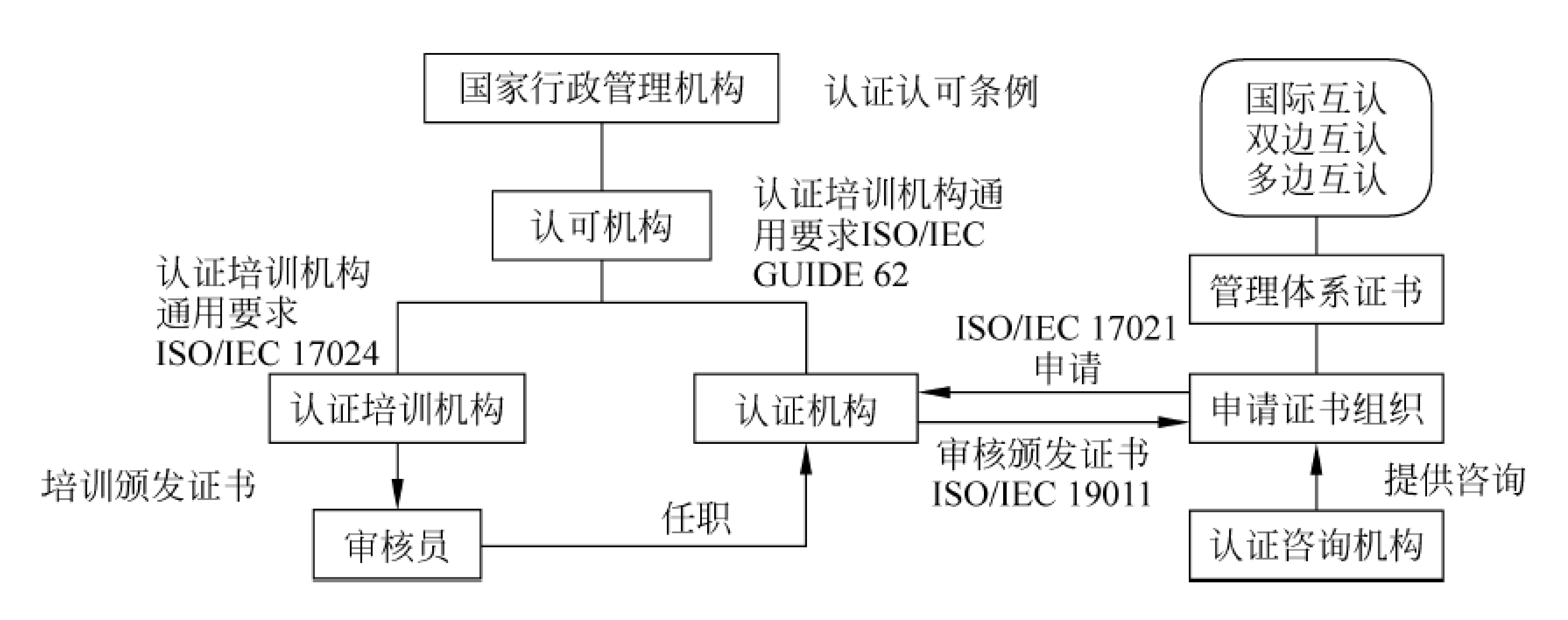


图 2-2　管理体系产业链

2.1.2　PDCA 模型

1. PDCA 循环简介

信息安全管理是指导和控制组织关于信息安全风险的相互协调的活动。首先应该制定信息安全的策略方针，它是信息安全管理的导向和支持，在此基础上选择控制目标与控制方式，企业和组织还需考虑控制成本与风险平衡的原则，将风险降低到组织可接受的水平，整个管理过程需要全员的参与，实施动态管理。实施安全管理，还应遵循管理的一般模式——PDCA 模型。

信息安全管理体系的实施、维护是一个持续改进的过程。PDCA 图可形象地说明系统的改进活动是周而复始的、不断循环的持续过程。PDCA 的含义是：

P(Plan)——计划，确定方针和目标，确定活动计划。

D(Do)——实施，采取实际措施，实现计划中的内容。

C(Check)——检查，检查并总结执行计划的结果，评价效果，找出问题。

A(Action)——行动，对检查总结的结果进行处理，成功的经验加以肯定并适当推广、标准化；失败的教训加以总结，以免重现；未解决的问题放到下一个 PDCA 循环。

每完成一个循环，ISMS 的有效性就上一个台阶。组织通过持续执行 PDCA 过程而使自身的信息安全水平得到不断提高，如图 2-3 所示。

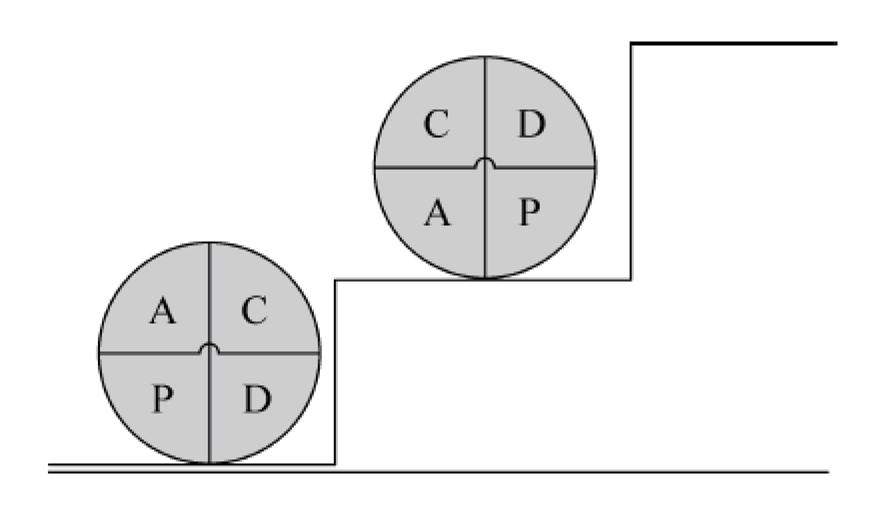


图 2-3　持续改进的 PDCA 模型

PDCA 循环的 4 个阶段可细分为 8 个步骤，每个步骤的具体内容如下。

计划阶段：制定具体工作计划，提出总体目标。进一步可分为以下 4 个步骤：

(1) 分析目前现状，找出存在的问题。

(2) 分析产生问题的各种原因以及影响因素。

(3) 分析并找出管理中的主要问题。

(4) 制定管理计划，确定管理要点。

根据管理中出现的主要问题，制定管理的措施、方案，明确管理的重点。制定管理方案时要注意整体的详尽性、多选性、全面性。

(5) 实施阶段：按照制定的方案执行。

在管理工作中全面执行制定的方案。制定的管理方案在管理工作中执行的情况，直接影响全过程。所以在实施阶段要坚决按照制定的方案去执行。

(6) 检查阶段：检查实施计划的结果。

检查工作，调查效果。这一阶段是比较重要的一个阶段，是对实施方案是否合理、是否可行、有何不妥的检查。它是检验上一阶段工作好坏的检验期，为下一阶段工作提供条件。

处理阶段：根据调查效果进行处理。进一步可分为以下两个步骤：

(7) 对已解决的问题，加以标准化。把已成功的可行的条文进行标准化，将这些纳入到制度、规定中，防止以后再发生类似问题。

(8) 找出尚未解决的问题，转入下一个循环中去，以便解决。

组织通过使用安全方针、安全目标、审核结果，利用对监控事件的分析、纠正和预防行动以及管理评审的信息，来持续改进 ISMS 的有效性。

PDCA 循环实际上是有效地进行任何一项工作的合乎逻辑的工作程序。在质量管理中，PDCA 循环得到了广泛的应用，并取得了很好的效果，因此有人称 PDCA 循环是质量管理的基本方法。之所以将其称为 PDCA 循环，是因为这 4 个过程不是运行一次就完结，而是要周而复始地进行。其特点是“大环套小环，一环扣一环，小环保大环，推动大循环”，每个循环系统包括 PDCA 4 个阶段，要周而复始地运动。PDCA 循环是螺旋式上升和发展的，每循环一次，要求提高一步。

实际上建立和管理信息安全管理体系和其他管理体系一样，需要采用过程的方法开发、实施和改进组织 ISMS 的有效性。信息安全管理体系的 PDCA 过程如图 2-4 所示。

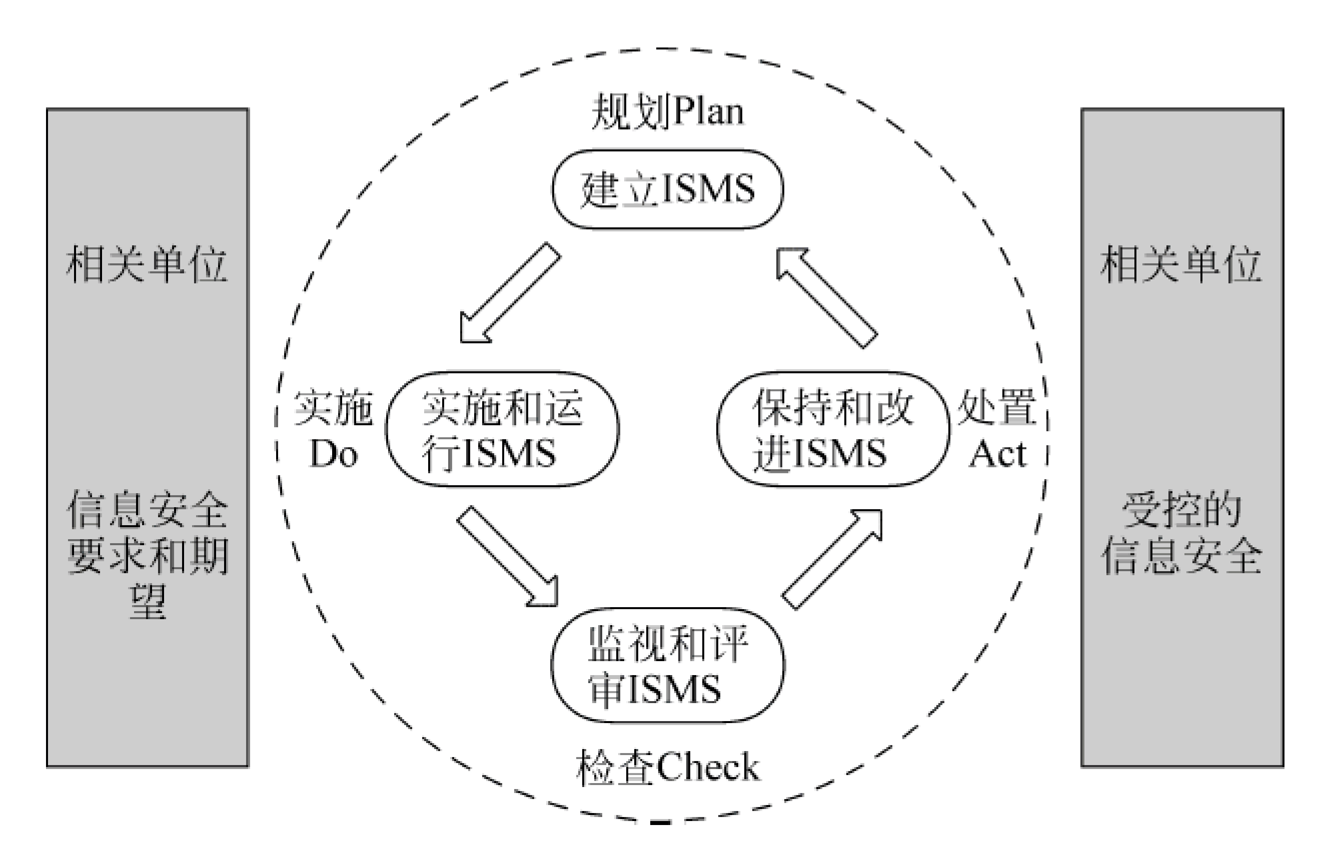


图 2-4　ISMS 的 PDCA 过程

ISMS 的 PDCA 具有以下内容：

1) 计划和实施

计划阶段用来保证 ISMS 的内容和范围被正确建立，信息安全风险被正确评估，处理这些风险的计划被有效开发。实施阶段用来实施在计划阶段确定的决策和解决方案。

2) 检查和行动

检查和行动阶段用来加强、修改和改进已识别和实施的信息安全方案。检查评审可以在任何时间、以任何频率实施。至于“怎样做”要考虑具体情况，在一些体系中可能需要建立

计算机化的过程来自动检测和响应安全事件；而其他的一些过程可能只需在信息安全事件发生时、被保护的信息资产变化时或威胁和脆弱性变化时，才做出必要的响应；需要进行周期性评审或审核以保证整个管理体系达成其目标并持续有效。

下面将详细描述 ISMS 的 PDCA 各阶段的特点。

2. 计划阶段

本阶段的主要任务是根据风险评估、法律法规要求、组织业务运营自身要求，来确定控制目标与控制方式。目的是保证正确地建立 ISMS 的内容和范围、识别和评估所有的信息安全风险，并开发合适的处理风险的计划。应该注意的是：计划活动及所有工作必须文件化，以作为管理变化的追溯。在计划阶段组织需要完成以下几方面的工作。

1）确定信息安全方针

在计划阶段要求组织和其管理层确定信息安全方针，包括组织的目标和目的框架、总体方向的建立和信息安全行动原则。

2）确定信息安全管理体系的范围

如果信息安全管理体系的范围只包括组织的某些部分时，要清楚地识别系统的从属关系、与其他系统接口、系统的边界。确定信息安全管理体系范围的文件应包括：

（1）建立范围的过程和信息安全管理体系的环境。

（2）组织战略及业务环境。

（3）组织使用的信息安全风险管理的方法。

（4）信息安全风险评价标准和所需的保护程度。

（5）在信息安全管理体系的范围内信息资产的识别。

3）制定风险识别和评估计划

风险评估文件应解释组织选择哪一种识别、评估风险的方法，为什么选择此方法，组织所处的业务环境，组织业务的大小和组织面临的风险等。文件也应包括组织选择的工具和技术，解释为什么它们适用于本组织信息安全管理体系的范围和风险，怎样正确地使用这些工具和技术以产生有效的结果。以下风险评估的详细内容应记录在文件内：

（1）信息安全管理体系范围内的资产评估，估价量度的使用信息。

（2）识别威胁和脆弱点。

（3）对威胁利用脆弱点的评估，及当此类事故发生时的影响。

（4）在评估结果的基础上计算风险，识别残余风险。

4）制定风险控制计划

组织应建立有详细日程安排的风险控制计划，对于识别的每一个风险都确定以下 4 点：

（1）选择处理风险的方法。

（2）已有的控制措施。

（3）建议新添的控制措施。

（4）实施新建议的控制措施的时间期限。

应识别出组织可接受的风险水平，选择合适的措施：

（1）决定接受风险，如不能采取其他措施或成本昂贵。

（2）规避风险。

（3）转移风险。

（4）降低风险到可接受的水平。

3．实施阶段

本阶段的主要目标是实施组织所选择的控制目标和控制措施，需要做的有以下几点：

1）保证安全、提供培训、提高安全意识

应该为信息安全管理体系的运行和所有安全控制措施的实施提供充足资源，提供实施所有控制措施的相关文件，并对信息安全管理体系文件进行维护；还应该进行信息安全教育活动，以提高员工安全意识，在组织中产生良好的风险管理和安全的文化；并对员工进行有关信息安全技能与技术的培训，使员工掌握信息安全的实现手段。

2）风险处理

对于经过评估可接受的风险，不需要进一步的措施。对于经过评估不可接受的风险，可以采取降低风险或风险转移等方法进行风险处理。如果决定转移风险，应该采取签订合同，参加保险的方式，或采取灵活组织结构（如找合作、合资伙伴）等进一步行动。无论哪一种情况，都必须保证风险转移到的组织能理解风险的性质，并且能够有效地管理这些风险。如果组织决定降低风险，就要在 ISMS 范围内实施已选择的降低风险的措施。实施的这些措施应与在计划活动中准备的风险控制计划相一致。

成功实施该计划要求有效的管理体系，管理体系定义了选择的措施目标与控制措施，落实责任和控制的过程，以及监控这些控制的过程。当一个组织决定接受高于可接受水平的风险时，应获得管理层的批准。在不可接受风险被降低或转移之后，还会有残余风险，控制措施应保证残余风险所产生的影响或破坏能及时被识别并适当管理。

4．检查阶段

本阶段的主要任务是进行有关方针、标准、法律法规与程序的符合性检查，对存在的问题采取措施，予以改进。检查阶段的目的是保证控制措施有效运行。另外，应该考虑风险评估的对象及范围的变化情况，如果发现风险控制措施不够充分，就必须决定采取必要的纠正措施，此类活动的实行应在 PDCA 循环的行动阶段。但要注意，纠正措施不能滥用，只有在必要时才采用。在下面这两种情况下要采用纠正措施。

（1）为了维护信息安全管理体系文件内部的一致性。

（2）如果进行改变，会使组织暴露于不可接受的风险之中。

检查活动应该对采用的控制措施与实施过程进行描述，内容包括：对风险的不间断评审，在技术、威胁或功能不断变化的情况下，对处理风险的方法和过程的调整。

在确定当前安全状态令人满意的同时，应注意技术的变化、业务的需求与新威胁和脆弱点的出现，尽量预测信息安全管理体系将来的变化，并采取有效措施确保其在将来持续有效地运转。

在检查阶段采集的信息应该可以用来测量信息安全管理体系，判断是否符合组织的安全方针和控制目标的有效性。常用的检查措施有以下几个。

（1）日常检查：这些程序应作为正式的业务过程经常进行，并设计用来侦测处理结果的错误。

（2）自治程序：自治程序是一种为了保证任何错误或失败在发生时能够被及时发现而建立的控制措施。例如，网络的设备发生故障或错误，监控程序或监控设备可以自动报警。

（3）从他处学习：这种学习适用于技术和管理活动，通过调查学习其他组织在处理此类问题时更好的办法来提高组织自身的能力。

（4）内部信息安全管理体系审核：通过在一个特定的常规审核时间段内检查信息安全管理体系所有的方面是否达到预想的效果，通常时间间隔不应该超过一年。

（5）管理评审：管理评审的目的是检查信息安全管理体系的有效性，以识别需要的改进和采取的行动。管理评审至少每年进行一次。

（6）趋势分析：经常进行趋势分析有助于组织识别需要改进的领域，并建立一个持续改进和循环提高的基础。

5. 改进阶段

本阶段的主要任务是对信息安全管理体系进行评价，寻求改进的机会，采取相应的措施。为使信息安全管理体系持续有效，应以检查阶段采集的不符合项信息为基础，经常进行调整与改进。对信息安全管理体系所作的改变或下一步行动计划，要及时告知所有的相关方，并提供相应的培训。

1）不符合项

一个不符合项是指：

（1）缺少或缺乏有效地实施和维护一个或多个 ISMS 的要求。

（2）在有客观证据的基础上，引起对 ISMS 完成信息安全方针和组织安全目标的能力的重大怀疑。

检查阶段的评审强调对于不符合项应采取进一步的调查，以识别事故的原因，采取的措施不仅要解决问题，而且要减少或防止此类问题的再次发生。

2）纠正和预防措施

应采取纠正措施以消除不符合项和其他违反标准要求的情况；应采取预防措施消除潜在不符合项的原因或其他可能的潜在违反标准要求的情况，以防止再次发生。

永远不可能全部消除孤立的不符合项，同时，孤立的事件可能事实上是一个安全弱点的征兆，如果不加以处理可能会对整个组织发生影响。当识别和实施任何纠正措施时，应从这种角度来考虑孤立事件。确保补救工作能预防和减少类似事件的再次发生。

2.1.3 建立信息安全管理体系的流程概述

组织应根据整体业务活动和风险，建立、实施、运行、监视、评审、保持并改进文件化的信息安全管理体系。不同的组织在建立与完善信息安全管理体系时，可根据自己的特点和具体的情况，采取不同的步骤和方法。但总体来说，建立信息安全管理体系一般要经过下列 6 个基本步骤：

（1）信息安全管理体系的策划与准备。

（2）信息安全管理体系文件的编制。

（3）建立信息安全管理框架。

(4) 信息安全管理体系的运行。

(5) 信息安全管理体系的审核。

(6) 信息安全管理体系的管理评审。

信息安全管理体系一旦建立,组织应当按照体系的规定要求进行运作,保持体系运行的有效性。信息安全管理体系应形成一定的文件,即应建立并保持一个文件化的信息安全管理体系,其中应阐述被保护的资产、风险管理方法、控制目标与控制措施、信息资产需要保护的程度等内容。

总之,通过参照信息安全管理模型,按照先进的信息安全管理标准建立完整的信息安全管理体系,并加以实施和保持,实现动态的、系统的、全员参与、制度化的、以预防为主的管理方式,以最低的成本、达到可接受的信息安全水平,从根本上为业务提供信息安全保障。

2.1.4 信息安全管理体系与 PDCA 循环

一般认为整个 ISO/IEC 27001 是一个 PDCA 循环,其本身又是许多循环的嵌套,如图 2-5 所示。

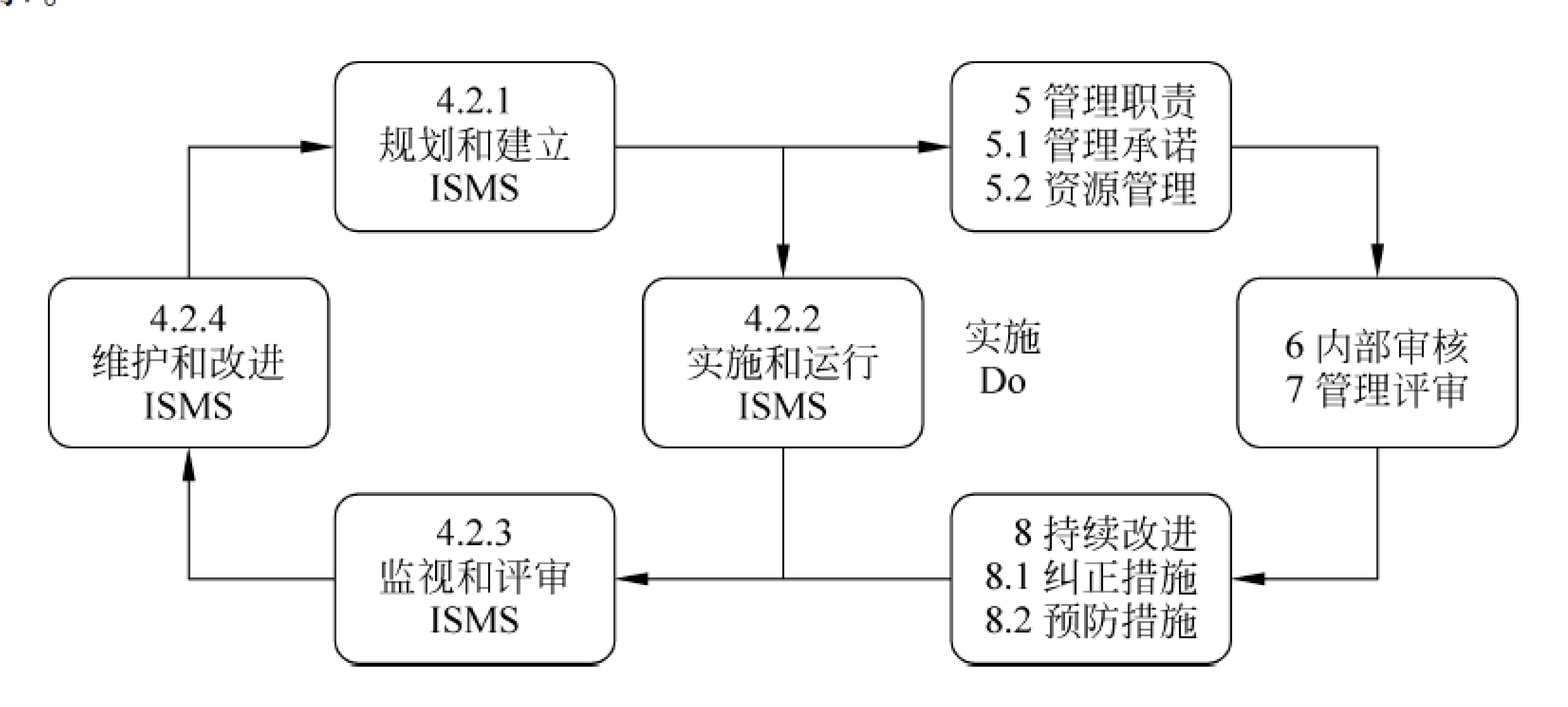


图 2-5 两个 PDCA 循环

表 2-1 给出了 PDCA 循环对应建立 ISMS 的过程中各阶段的工作内容。

表 2-1 ISMS 计划

阶段	阶段工作内容
准备和启动阶段	1. 识别信息安全要求,进行差距分析 2. 制定项目工作计划,明确项目时间表 3. ISMS 培训,包括全员意识培训、标准要求培训、风险评估培训
规划(建立)	1. 制定信息安全方针和范围 2. 编制风险评估程序文件 3. 执行风险评估 4. 编制风险处理计划 5. 编制 SoA(适用声明)文件 6. 编制 ISO/IEC27001 中 4.3.1 要求的其他相关 ISMS 文件 7. ISO/IEC27001 涉及的信息安全技术控制措施的方案设计、评审(可选) 8. 组织提出的特定的信息安全技术控制措施的方案设计、评审(可选)

续表

阶　段	阶段工作内容
实施(实施和运行)	1. 批准 ISMS 文件并颁布实施 2. 对 ISMS 文件开展宣传贯彻和培训 3. 确保承担信息安全职责的员工按照 ISMS 文件要求执行
检查(监视和评审)	1. 编制控制措施有效性测量程序 2. 实施检查和测量 3. 内审员培训和执行内部审核 4. 执行管理评审
改进(持续改进)	1. 采取预防措施(可选) 2. 采取纠正措施(可选) 3. 采取措施,持续改进 ISMS

2.2 信息安全管理相关标准

2.2.1 国外信息安全管理相关标准

1. ISO/IEC 13335

ISO/IEC 13335 是国际标准《IT 安全管理指南》,英文名称为 Guidelines for the Management of IT Security(GMITS)。该标准由 5 个部分组成,分别如下。

(1) ISO/IEC TR 13335-1：1996《信息技术　信息技术安全管理指南　第 1 部分　信息技术安全概念和模型》

本部分提供基本的管理概念和模型。这些概念和模型是后续标准进一步讨论和开发 IT 安全管理的基础,本部分对完整理解 ISO/IEC TR 13335 的以下部分非常重要。

(2) ISO/IEC TR 13335-2：1997《信息技术　信息技术安全管理指南　第 2 部分　管理和规划信息技术安全》

本部分描述了管理和计划方面的内容。它涉及组织 IT 系统管理相关职责的人员,包括负责 IT 系统设计、实施、测试、采购、操作的人员,以及那些负责组织信息化的管理人员。

(3) ISO/IEC TR 13335-3：1998《IT 安全管理技术》

本部分描述项目生命周期内 IT 安全管理相关的技巧。包括项目的规划、设计、实施、测试、采购和操作等过程相关的技巧。这些技巧可以用来评估组织的 IT 安全风险,帮助组织建立和维持合适级别的安全控制。

(4) ISO/IEC TR 13335-4：2000《安全措施的选择》

本部分在安全控制措施的选择方面提供了指南,指导组织如何根据第三部分所提到的风险评估的结果,选择适合组织的控制,并对采取的控制进行进一步的评估,以评价其效果。

(5) ISO/IEC TR 13335-5：2001《网络安全管理指南》

本部分针对网络和通信的安全管理提供了指南,指导组织从哪些方面来识别和分析计算机网络和通信系统相关的 IT 安全要求,同时概括介绍了可供采用的安全对策。

2．AS/NZS 4036

AS/NZS 4360：1999 是澳大利亚和新西兰联合开发的风险管理标准，第一版于 1995 年发布。该标准广泛应用于新南威尔士洲、澳大利亚政府、英联邦卫生组织等机构。在 AS/NZS 4360：1999 中，风险管理分为建立环境、风险识别、风险分析、风险评价、风险处置、风险监控与回顾、通信和咨询 7 个步骤，AS/NZS 4360 界定的风险管理程序如图 2-6 所示。

1992 年，澳大利亚标准委员会和新西兰标准委员会成立联合技术委员会，其 31 个成员分别由代表来自 22 个行业、专业和各级政府组织的专家组成。经过广泛的信息搜集、整理和讨论，并多次修改，于 1995 年制定和出版了世界上第一个“国家”风险管理标准：澳大利亚/新西兰风险管理标准（AS/NZS 4360：1995），并于 1999 年重新修订。该标准的特点是实用范围广泛，为各行业各部门的风险管理提供了一个共同框架，被澳大利亚和新西兰的公共部门和私人企业单位广泛采纳，并在世界其他国家和地区广受欢迎，在澳大利亚三千多个标准中销路最好。该标准于 1996 年稍微改动后成为国际电工委员会（IEC）推荐使用标准。

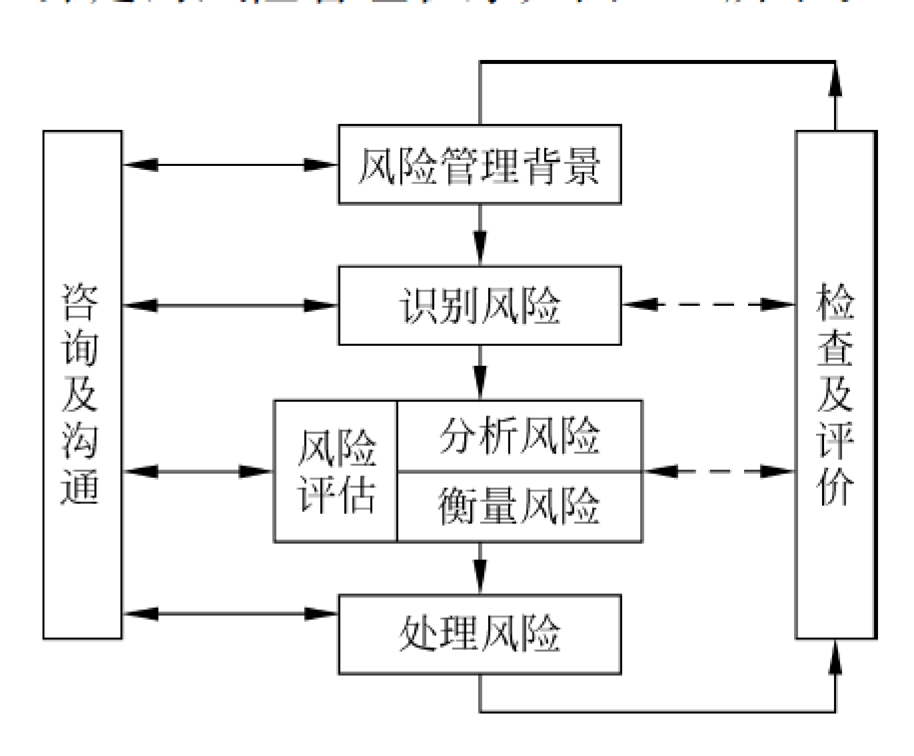


图 2-6　AS/NZS 4360 风险管理程序

澳洲风险标准（AS/ NZS 4360）的正文包括 5 个部分：一是应用范围与概念；二是风险管理要求；三是风险管理概论；四是风险管理步骤；五是风险管理记录和档案。另外 7 个附件为风险管理实际操作提供了一套适合于各种机构和个人风险管理的方法和程序，满足了综合风险管理的需求。为适应此要求，特别将风险的概念拓展为“一个事件发生的概率与影响的组合。风险是预期的背离，可以有正反双向的作用，而事件的发生可以是确定或不确定、一个或多个、单独发生或与其他事件一起发生”。风险管理是“针对潜在机会及不良影响的有效管理的文化、程序和框架”。

3．ITBPM

IT 基准安全防护手册（IT Baseline Protection Manual，ITBPM）是德国联邦信息安全局召集信息安全专家共同编撰的信息安全防护准则，采用手册的形式为典型 IT 系统提供了一套完整的安全防护建议，其目标不仅要保证 IT 系统处于合理且充分满足一般安全防护需求的水平，并且为 IT 系统及其应用系统提升安全防护等级做好必要准备。

ITBPM 比其他信息安全管理系统标准更加详细地对威胁和安全措施加以分类，具体详细地罗列出信息资产清单、威胁清单和安全措施清单。依照其分类方式，首先对信息资产划分层次后再分割为若干模块，然后分析每一模块面临的威胁，最后对每一模块提供一系列可行且有效的安全防护措施建议。用户依据这些建议建立信息安全机制，即可满足基本的安全防护要求，有效保护信息资产的安全。如果用户有进一步的安全等级需求，可以再进行更深层次的风险评估工作，增加必要的安全防护措施以提高信息资产的安全防护水平。在整个信息资产风险评估过程中，用户只需要将组织内部的潜在风险与 ITBPM 的威胁项目检

查表进行对照就能够完成必要的风险评估工作,不仅大大简化了评估过程并使用户对每个潜在安全风险一目了然。

将 ITBPM 应用于 IT 系统的信息安全防护一般通过 5 个步骤完成:绘制整个 IT 系统的资产构架,包括一般部件资产、基础设施资产、IT 系统特定资产等;分析资产面临的威胁,包括每个资产的一般性描述,存在的潜在威胁;分析威胁对应的安全措施,依据威胁分类进行安全措施分类,包括各项防护措施的安全防护等级和具体操作的详细描述;列举 IT 系统现有防护措施清单;对比现有防护措施和建议防护措施,实施防护措施从而满足 IT 系统信息安全的基准防护要求。

4. NIST SP800-39

SP800-39:2011 是美国国家标准和技术研究院(简称 NIST)在 FISMA(the Federal Information Security Management Act of 2002,联邦信息安全管理法案)项目实施中产生的重要标准之一,是支撑 FIMSA 项目实施系列标准的旗舰性文件,是其他标准的重要基础和指导。该标准主要为联邦信息系统和组织提供了开展风险管理行动的过程方法,提出了一个三层的风险管理层次结构,并详细介绍了联邦政府如何将风险管理过程应用到风险管理结构的三个层次。

该标准与下列一系列管理信息安全风险有关的安全标准和指南一起,为联邦政府统一的信息安全框架提供支撑。

(1) SP800-37:联邦信息系统风险管理框架应用指南。

(2) SP800-53:推荐的联邦信息系统和组织安全控制措施。

(3) SP800-53A:评估联邦信息系统和组织的安全控制措施及建立有效的安全评估计划指南。

(4) SP800-30:风险评估实施指南。

同时,国际标准组织(ISO)和国际电工委员会(IEC)也发布了下列风险管理和信息安全标准。

(1) ISO/IEC 31000:风险管理-准则和指南。

(2) ISO/IEC 31010:风险管理-风险评估技术。

(3) ISO/IEC 27001:信息技术-安全技术-信息安全管理体系　要求。

(4) ISO/IEC 27005:信息技术-安全技术-信息安全风险管理。

为了在组织内部整合风险管理过程,该标准给出了一个三层风险管理架构:组织层、使命/业务过程层、信息系统层。组织通过在这三个层面实施风险管理过程,将会实现其持续改进风险相关活动的目标,并实施与所有利益相关方之间有效的层间和层内的沟通,如图 2-7 所示。

风险管理是一个广泛过程,要求组织开展以下方面的活动:①明确要执行的风险管理活动的背景(例如,风险框架);②评估风险;③对风险做出响应;④通过使用有效的组织间的沟通和反馈的信息流不断改进组织与风险相关的活动,持续监控风险。

风险管理的第一步阐述了如何确定风险框架或确定风险背景,也就是说,给出风险决策所处的环境。风险管理的第二步阐述了组织如何评估已确定风险框架内的风险。风险管理的第三步阐述了组织应如何响应风险。风险管理的第四步阐述了组织应如何持续监视风

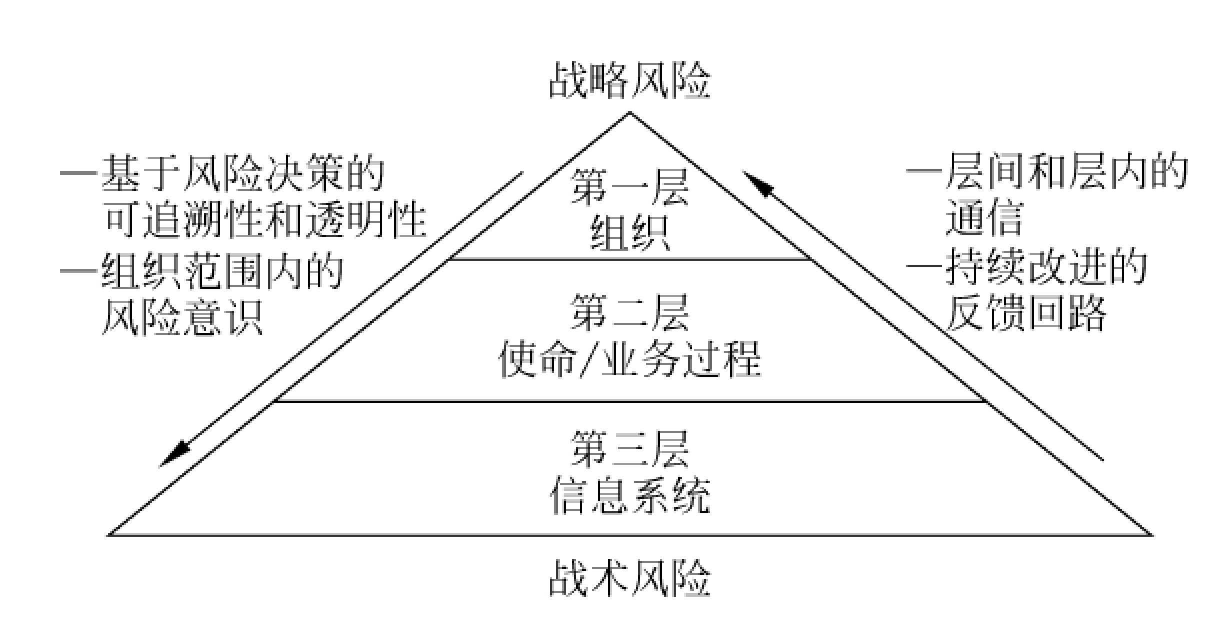


图 2-7　风险管理层次结构

险。结合风险管理的 4 个步骤、风险管理的三层结构以及相关任务，表 2-2 汇总了风险管理过程中涉及的所有任务。

表 2-2　风险管理过程中的任务汇总

步骤 1：风险框架	
任务 1-1　风险假设	确定组织内部影响评估、应对以及检测风险的方式
任务 1-2　风险约束条件	确定执行风险评估、风险应对、风险监测活动时的约束条件
任务 1-3　风险承受力	确定组织风险承受力的水平
任务 1-4　重要事务和协议	确定用于管理风险时组织要考虑的重要事务和协议
步骤 2：风险评估	
任务 2-1　威胁和漏洞识别	识别对组织内部信息系统以及系统运行环境的威胁和自身漏洞
任务 2-2　风险决策	在已发现的威胁利用已发现的漏洞时，确定针对组织运行和资产、个人、其他组织和国家的风险
步骤 3：风险响应	
任务 3-1　风险响应识别	识别可选择的行动过程，以响应在风险评估过程中发现的风险
任务 3-2　对可选方法的评估	评估可选的活动过程用以响应风险
任务 3-3　风险响应决策	决定适当的活动过程来响应风险
任务 3-4　风险响应实施	实施已选择的活动过程来响应风险
步骤 4：风险监视	
任务 4-1　风险监视策略	为组织开发一个风险监视策略，包括监测活动的目的、类型、频率
任务 4-2　风险监视	监视组织信息系统和运行环境，并基于一个持续的平台确认保证风险响应策略的有效性，同时识别变化

5．ISO/IEC 27000

ISO/IEC 27000 信息安全管理体系、基础和术语提供了 ISMS 标准族中所涉及的通用术语及基本原则，是 ISMS 标准族中最基础的标准之一。ISMS 标准族中的每个标准都有“术语和定义”部分，但不同标准的术语间往往缺乏协调性，而 ISO/IEC 27000 则主要用于实现这种协调。

ISMS 的概念最初来源于 ISO/IEC 17799 的前身 BS 7799，随着其作为国际标准发布和普及被广泛接受。

ISO/IEC JTC1/SC27/WG1(国际标准化组织/国际电工委员会信息技术委员会/安全

技术分委员会/第一工作组)是制定和修订 ISMS 标准的国际组织。

图 2-8 是该标准的发展历程。

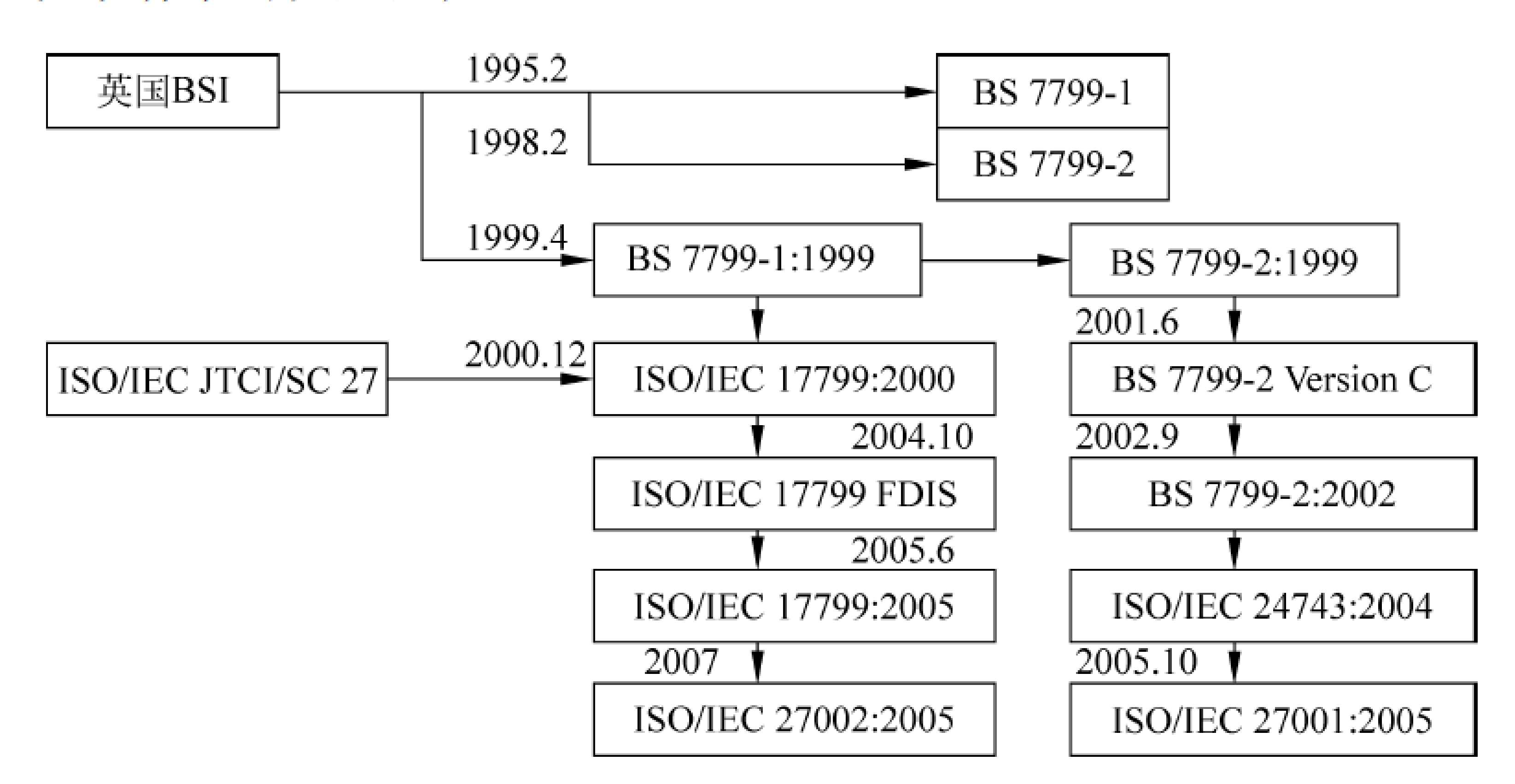


图 2-8　ISO/IEC 27001：2005 发展过程

ISO/IEC 27000 族标准是国际标准化组织专门为 ISMS 预留下来的一系列相关标准的总称。具体如下：

ISO/IEC 27000 信息安全管理体系基础和术语。

ISO/IEC 27001 信息安全管理体系要求。

ISO/IEC 27002 信息安全管理实用规则。

ISO/IEC 27003 信息安全管理体系实施指南。

ISO/IEC 27004 信息安全管理测量。

ISO/IEC 27005 信息安全风险管理。

ISO/IEC 27006 信息安全体系认证机构的认可要求。

ISO/IEC 27007 信息安全管理体系审核指南。

ISO/IEC 27008 信息安全管理体系技术审核。

下列编号可能会是分行业的应用：

ISO/IEC 27009 工业和政府的部门间的协作和交流。

ISO/IEC 27011 电信业信息安全管理指南。

ISO/IEC 27012(电子政务服务信息安全管理指南)。

ISO/IEC 27013(未定,讨论中)。

下列编号可能会仅涉及某个具体的安全领域。

ISO/IEC 27031 业务连续性 ICT 就绪规范。

ISO/IEC 27032 网际安全指南。

ISO/IEC 27033 网络安全。

ISO/IEC 27034 应用安全指南。

ISO/IEC 27035 信息安全事件管理。

编号可能会一直预留至 ISO/IEC 27059,但下列标准编号不同于 ISO/IEC 27000 族：

ISO/IEC 27799 健康领域的安全管理。

ISO/IEC TR 13569 银行业信息安全指南。

2.2.2　国内信息安全管理相关标准

1. GB 17895—1999

GB 17895—1999 是计算机信息系统安全保护等级划分准则,标准规定了计算机系统安全保护能力的 5 个等级,即:第一级　用户自主保护级;第二级　系统审计保护级;第三级　安全标记保护级;第四级　结构化保护级;第五级　访问验证保护级。

本标准适用计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高,逐渐增强。

1) 第一级　用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据,使用户具备自主安全保护的能力。它具有多种形式的控制能力,对用户实施访问控制,即为用户提供可行的手段,保护用户和用户组信息,避免其他用户对数据的非法读写与破坏。

2) 第二级　系统审计保护级

与用户自主保护级相比,本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制,它通过登录规程、审计安全性相关事件和隔离资源,使用户对自己的行为负责。

3) 第三级　安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外,还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述;具有准确地标记输出信息的能力;可消除通过测试发现的任何错误。

4) 第四级　结构化保护级

本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上,它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外,还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义,使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制;支持系统管理员和操作员的职能;提供可信设施管理;增强了配置管理控制。系统具有相当强的抗渗透能力。

5) 第五级　访问验证保护级

本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的;必须足够小,能够分析和测试。为了满足访问监控器需求,计算机信息系统可信计算基在其构造时,排除那些对实施安全策略来说并非必要的代码;在设计和实现时,从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能;扩充审计机制,当发生与安全相关的事件时发出信号;提供系统恢复机制。系统具有很高的抗渗透能力。

2. GB/T 20269—2006

GB/T 20269—2006《信息安全技术　信息系统安全管理要求》依据 GB 17859—1999 的 5 个安全保护等级的划分,规定了信息系统安全所需要的各个安全等级的管理要求,适用于按等级划分要求进行的信息系统安全的管理。

3. GB/T 22239—2008

GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》是依据国家信息安全等级保护管理规定制定的、信息安全等级保护相关系列标准之一。与该标准相关的系列标准包括：GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》、国家标准《信息安全技术　信息系统安全等级保护实施指南》。该标准与 GB 17895—1999、GB/T 20269—2006、GB/T 20270—2006、GB/T 20271—2006 等标准共同构成了信息系统安全等级保护的相关配套标准。其中，GB 17895—1999 是基础性标准，本标准、GB/T 20269—2006、GB/T 20270—2006、GB/T 20271—2006 等是在 GB 17895—1999 基础上的进一步细化和扩展。该标准在 GB 17895—1999、GB/T 20269—2006、GB/T 20270—2006、GB/T 20271—2006 等技术类标准的基础上，根据现有技术的发展水平，提出和规定了不同安全保护等级信息系统的最低保护要求，即基本安全要求，基本安全要求包括基本技术要求和基本管理要求，该标准适用于指导不同安全保护等级信息系统的安全建设和监督管理。

2.3 信息安全管理工具

1. MBSA

Microsoft 基准安全分析器(MBSA)可以检查操作系统和 SQL Server 更新。MBSA 还可以扫描计算机上的不安全配置。检查 Windows 服务包和修补程序时，它将 Windows 组件、如 Internet 信息服务(IIS)和 COM＋也包括在内。MBSA 使用一个 XML 文件作为现有更新的清单。该 XML 文件包含在存档 Mssecure.cab 中，由 MBSA 在运行扫描时下载，也可以下载到本地计算机上，或通过网络服务器使用。

2. MSAT

微软安全评估工具(MSAT)是微软的一个风险评估工具，与 MBSA 直接扫描和评估系统不同，MSAT 通过填写的详细的问卷以及相关信息，MSAT 处理问卷反馈，并评估组织在诸如基础结构、应用程序、操作和人员等领域中的安全实践，然后提出相应的安全风险管理措施和意见。一般来说，如果说 MBSA 是个扫描器，则 MSAT 就是个风险评估工具。

3. COBRA

COBRA(Consultative，Objective and Bi-functional Risk Analysis)是英国的 C&A 系统安全公司推出的一套风险分析工具软件，它通过问卷的方式来采集和分析数据，并对组织的风险进行定性分析，最终的评估报告中包含已识别风险的水平和推荐措施。此外，COBRA 还支持基于知识的评估方法，可以将组织的安全现状与 ISO 17799 标准相比较，从中找出差距，提出弥补措施。

4. CRAMM

CRAMM(CCTA Risk Analysis and Management Method)是由英国政府的中央计算

机与电信局(Central Computer and Telecommunications Agency,CCTA)于1985年开发的一种定量风险分析工具,同时支持定性分析。经过多次版本更新,目前由Insight咨询公司负责管理和授权。CRAMM是一种可以评估信息系统风险并确定恰当对策的结构化方法,适用于各种类型的信息系统和网络,也可以在信息系统生命周期的各个阶段使用。CRAMM的安全模型数据库基于著名的"资产/威胁/弱点"模型,评估过程经过资产识别与评价、威胁和弱点评估、选择合适的推荐对策这三个阶段。CRAMM与BS 7799标准保持一致,它提供的可供选择的安全控制多达3000个。除了风险评估,CRAMM还可以对符合ITIL(IT Infrastructure Library)指南的业务连续性管理提供支持。

5. ASSET

ASSET(Automated Security Self-Evaluation Tool)是美国国家标准技术协会(National Institute of Standard and Technology,NIST)发布的一个可用来进行安全风险自我评估的自动化工具,它采用典型的基于知识的分析方法,利用问卷方式来评估系统安全现状与NIST SP800-26指南之间的差距。NIST Special Publication 800-26,即信息技术系统安全自我评估指南(Security Self-Assessment Guide for Information Technology Systems),为组织进行信息系统风险评估提供了众多控制目标和建议技术。

6. RiskWatch

美国RiskWatch公司综合各类相关标准,开发了风险分析自动化软件系统,进行风险评估和风险管理,共包括5类产品,分别针对信息系统安全、物理安全、HIPAA标准、RW17799标准、港口和海运安全。RiskWatch工具具有以下特点:友好的用户界面;预定义的风险分析模板,给用户提供高效、省时的风险分析和脆弱性评估;数据关联功能;经过证明的风险分析模型。

7. CORA

CORA(Cost-of-Risk Analysis)是由国际安全技术公司(International Security Technology)开发的一种风险管理决策支持系统,它采用典型的定量分析方法,可以方便地采集、组织、分析并存储风险数据,为组织的风险管理决策支持提供准确的依据。

思考题

1. 解释信息安全管理体系模型的主要内容。
2. 论述信息安全管理体系的PDCA过程。
3. 叙述建立信息安全管理体系的流程。
4. 查阅资料,归纳国内信息安全管理相关标准。
5. 查阅资料,归纳ISO/IEC 27000信息安全管理体系系列相关标准。
6. 查阅资料,归纳信息安全管理工具。

第3章 信息安全风险评估的主要内容

3.1 信息安全风险评估工作概述

3.1.1 风险评估依据

风险评估依据国家政策法规、技术规范与管理要求、行业标准或国际标准进行，其依据主要包括：

1. 政策法规

国家信息化领导小组关于加强信息安全保障工作的意见(中办发[2003]27 号)。

2. 国际标准

(1) ISO/IEC 27001：2005 信息安全管理体系 要求。

(2) ISO/IEC 27002：2005 信息安全管理实用规则。

(3) ISO/IEC TR 13335 信息技术安全管理指南。

(4) SSE-CMM 系统安全工程能力成熟模型。

3. 国家标准

(1) GB/T 20984—2007 信息安全技术 信息安全风险评估规范。

(2) GB 17859—1999 计算机信息系统安全保护等级划分准则。

(3) GB/T 18336.1～18336.3—2001 信息技术 安全技术 信息技术安全性评估准则。

4. 行业通用标准

(1) CVE 公共漏洞数据库。

(2) 信息安全应急响应机构公布的漏洞。

(3) 国家信息安全主管部门公布的漏洞。

3.1.2 风险评估原则

通过风险评估有助于认清信息环境的安全状况，明确责任达成共识；有助于采取并完

善更加经济有效的安全保障措施；有助于保持信息安全策略的一致性和连续性，从而服务于国家信息化发展，促进信息安全保障体系的建设，提高信息系统的安全保障能力。

风险评估原则包括：可控性原则（人员可控性、工具可控性、项目过程可控性）；完整性原则；最小影响原则；保密原则。具体如下：

1. 可控性原则

1）人员可控性

所有参与信息安全风险评估的人员均应进行严格的资格审查和备案，明确其职责分工，并对人员工作岗位的变更执行严格的审批手续，确保人员可控。评估人员的安排需在评估工作说明中明确定义，并要得到双方的同意、确认。如果根据项目的具体情况，需要进行人员调整时，必须经过正规的项目变更程序，得到双方的正式认可和签署。

2）工具可控性

所使用的风险评估工具均应通过多方综合性能对比、精心挑选，并取得有关专家论证和相关部门的认证。评估工作中所使用的技术工具均事先通告评估对象，向评估对象介绍主要工具的使用方法并进行实验后方可使用。

3）项目过程可控性

评估项目管理将依据项目管理方法学，重视项目管理的沟通管理，达到项目过程的可控性。

2. 完整性原则

严格按照委托单位的评估要求和指定的范围进行全面的评估服务。

3. 最小影响原则

从项目管理层面和工具技术层面，力求将风险评估对信息系统的正常运行的可能影响降低到最低限度。

4. 保密原则

与评估对象签署保密协议和非侵害性协议。

3.1.3　风险评估组织管理

由于信息安全风险评估工作必然涉及系统当中的关键部分和核心信息，敏感性极强，如果处理不当，反而可能引入新的风险。因此，必须高度重视信息安全风险评估的组织管理工作。网络与信息系统的拥有、运营、使用单位和主管部门要按照“谁主管谁负责，谁运营谁负责”的原则，负起严格管理的责任。一方面，对评估者的技术水平要提出高要求；另一方面，参与信息安全风险评估工作的单位及有关人员必须遵守国家信息安全的有关法律法规，承担相应的责任和义务。风险评估工作的发起方必须采取相应保密措施，并与参与评估的有关单位或人员签订具有法律约束力的保密协议。对关系国计民生和社会稳定的基础信息网络和重要信息系统，信息安全风险评估工作必须遵循国家的有关规定。

信息系统风险评估的参与角色一般有主管机关、信息系统拥有者、信息系统承建者、信

息系统安全评估机构、信息系统的关联者(即因信息系统互联、信息交换和共享、系统采购等行为与该系统发生关联的机构)。他们在信息系统安全风险评估中的责任如表 3-1 所示。

表 3-1 风险评估中的角色和责任

角　色	责　任
主管机关	提出、制定并批准本部门的信息安全风险管理策略； 领导和组织本部门内的信息系统安全评估工作； 基于本部门内信息系统的特征以及风险评估的结果，判断信息系统残余风险是否可接受，并确定是否批准信息系统投入运行； 检查信息系统运行中产生的安全状态报告； 定期或不定期地开展新的信息安全风险评估工作
信息系统拥有者	制定安全计划，报主管机关审批； 组织实施信息系统自评估工作； 配合强制性检查评价或委托评估工作，并提供必要的文档等资源； 向主管机关提出新一轮风险评估的建议； 改善信息安全防护措施，控制信息安全风险
信息系统承建者	根据对信息系统建设方案的风险评估结果，修正安全方案，使安全方案成本合理、积极有效，在方案中有效地控制风险； 规范建设，减少在建设阶段引入的新风险； 确保安全组件产品得到了相关机构的认证
信息系统安全评估机构	提供独立的信息系统安全风险评价； 对信息系统中的安全防护措施进行评估，以判断： (1) 这些安全防护措施在特定运行环境中的有效性。 (2) 实现了这些措施后系统中存在的残余风险。 提出调整建议，以减少信息系统中的脆弱性，有效对抗安全威胁，控制风险； 保护风险评估中获得的敏感信息，防止被未授权的、无关人员和单位获得
信息系统的关联机构	遵守安全策略、法规、合同等涉及信息系统交互行为的安全要求，减少信息安全风险； 协助风险评估机构确定评估边界； 在风险评估中提供必要的资源和资料

3.2 风险评估基础模型

3.2.1 风险要素关系模型

要实施风险评估就必须对其要素有一个准确的理解，图 3-1 显示了风险评估的各要素及其关系。其中方框部分的内容为风险评估的基本要素，椭圆部分的内容是与这些要素相关的属性，也是风险评估要素的一部分。

图 3-1 中这些要素之间存在着以下关系：业务战略依赖于资产来完成；资产拥有价值，组织的业务战略越重要，对资产的依赖程度越高，资产的价值就越大；资产的价值越大，则

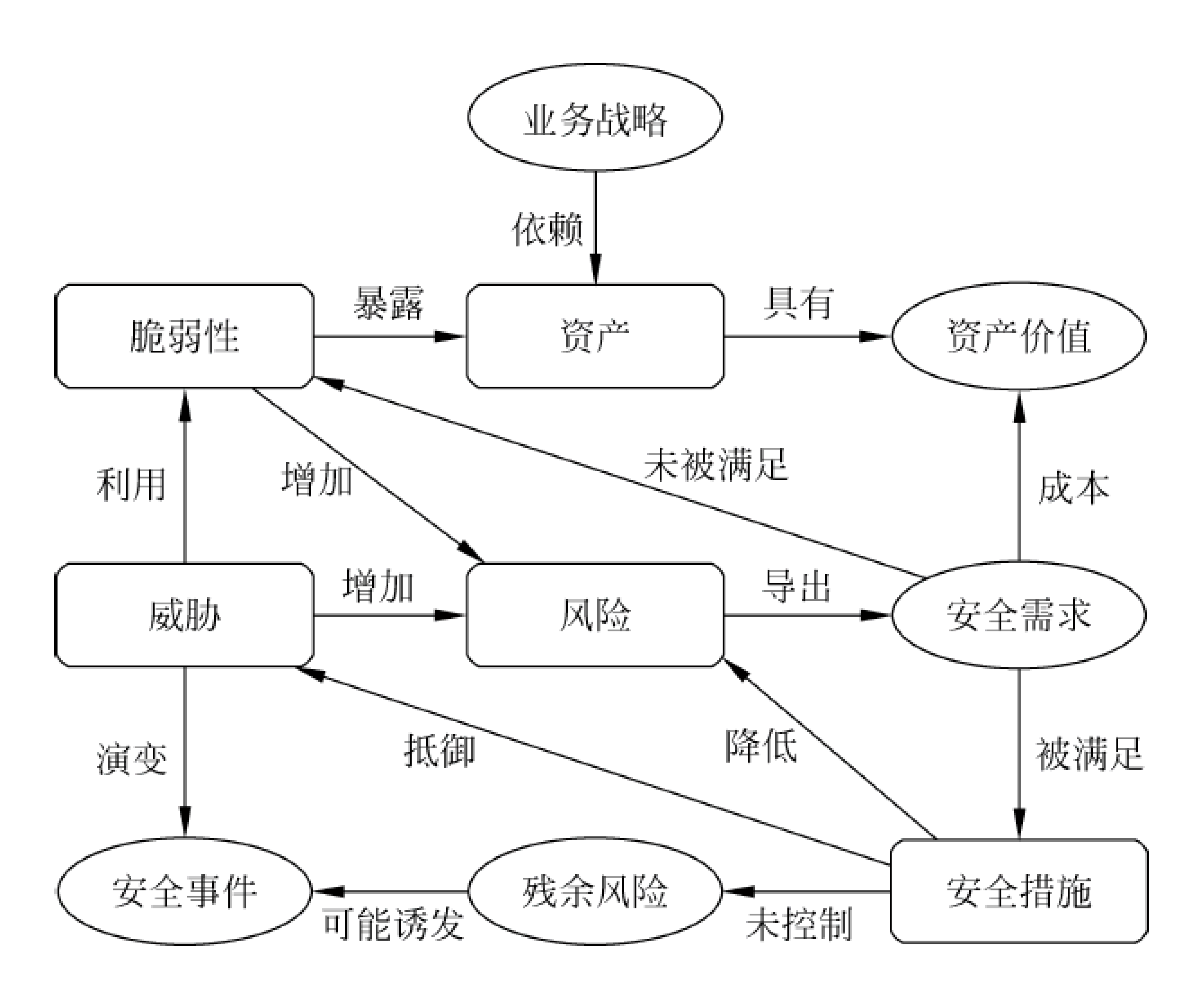


图 3-1　风险评估要素关系图

风险越大；风险是由威胁发起的，威胁越大则风险越大，并可能演变成安全事件；威胁需要利用脆弱性，脆弱性越大则风险越大；脆弱性使资产暴露，是未被满足的安全需求，威胁通过利用脆弱点危害资产，从而形成风险；资产的重要性和对风险的意识将会导出安全需求；安全需求要通过安全措施来得以满足，且是有成本的；安全措施可以抗击威胁，降低风险，减弱安全事件的影响；风险不可能、也没有必要降为零，在实施了安全措施后还会有残留的风险；部分残余风险来自于安全措施可能不当或无效，在以后需要继续控制这部分风险，另一部分残余风险则是在综合考虑了安全的成本与资产价值后，有意未去控制的风险，这部分风险是可以被接受的；残余风险应受到密切监视，因为它可能会在将来诱发新的安全事件。

下面主要参考 ISO/IEC TR 18044、ISO/IEC Guide 73：2002 等国际标准给出相关要素的定义。

资产是任何对组织有价值的事物。

信息安全事件(Event)是指识别出的发生的系统、服务或网络事件，表明可能违反信息安全策略或防护措施失效；或以前未知的与安全相关的情况。

信息安全事故(Incident)是指一个或一系列非期望的或非预期的信息安全事件，这些信息安全事件可能对业务运营造成严重影响或威胁信息安全。

残余风险：实施风险处置后仍旧残留的风险。

接受风险：接受风险的决策。

风险分析：系统地使用信息以识别来源和估计风险。

风险评估：风险分析和风险评价的全过程。

风险评价：将估计的风险与既定的风险准则进行比较以确定重要风险的过程。

风险管理：指导和控制一个组织风险的协调的活动。

风险处置：选择和实施措施以改变风险的过程。

控制目标和控制措施是基于风险评估和风险处理过程的结果和结论、法律法规要求、合

同业务和组织对信息安全的业务要求而确定的。

3.2.2 风险分析原理

风险分析原理如图 3-2 所示。

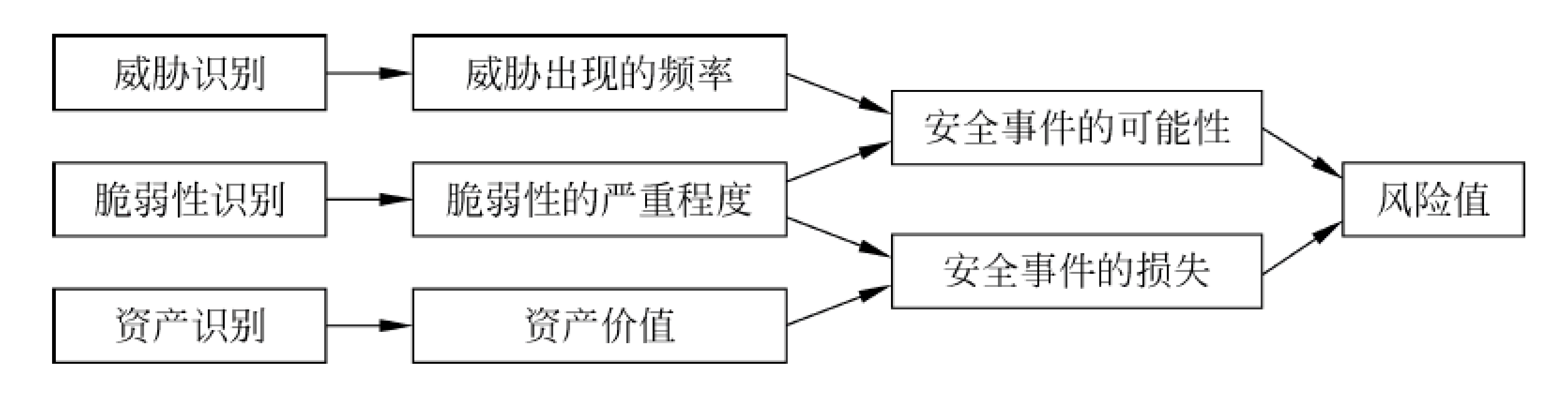


图 3-2 风险分析原理图

风险分析中要涉及资产、威胁、脆弱性等基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。风险分析的主要内容为：

（1）对资产进行识别，并对资产的价值进行赋值。

（2）对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值。

（3）对资产的脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值。

（4）根据威胁及威胁利用弱点的难易程度判断安全事件发生的可能性。

（5）根据脆弱性的严重程度及安全事件所作用资产的价值计算安全事件的损失。

（6）根据安全事件发生的可能性以及安全事件的损失，计算安全事件一旦发生对组织的影响，即风险值。

3.2.3 风险评估方法

评估方法的选择直接影响到信息系统安全风险评估过程中的每个环节，甚至可能影响最终的评估结果，因此需要根据系统的具体情况，选择合适的风险评估方法。风险评估的方法有很多种，概括起来可分为三大类：定性的风险评估方法、定量的风险评估方法、定性与定量相结合的评估方法。

1. 定性评估方法

定性评估方法是目前采用最为广泛的一种方法，它需要凭借评估分析者的经验、知识和直觉，结合标准和惯例，为风险评估要素的大小或高低程度定性分级，带有很强的主观性。定性分析的操作方法可以多种多样，包括小组讨论、检查列表、问卷、人员访谈、调查等。定性分析操作起来相对容易，但可能因为评估分析者在经验和直觉上的偏差而使分析结果失准。

常用的定性评估方法有：安全检查表法、专家评价法、事故树分析法、事件树分析法、潜在问题分析法、因果分析法、作业安全分析法等。

2. 定量评估方法

定量的评估方法对构成风险的各个要素和潜在损失的水平赋以数值或货币的金额，当

度量风险的所有要素(资产价值、威胁可能性、弱点利用程度、安全措施的效率和成本等)都被赋值以后,风险评估的整个过程和结果就可以进行量化。通过定量分析可以对安全风险进行准确的分级,能够获得很好的风险评估结果。但是,对安全风险进行准确分级的前提保证是可供参考的数据指标正确,而这个前提对于信息系统日益复杂多变的今天,是很难得到保证的。由于数据统计缺乏长期性,计算过程又极易出错,定量分析的细化非常困难,所以目前的风险评估分析很少完全只用定量的分析方法进行分析。

常用的定量评估方法有:层次分析法、模糊综合评判法、神经网络、灰色系统预测模型等。

3. 定量分析和定性分析方法的比较

定量的风险评估方法、定性的风险评估方法、定性与定量相结合的评估方法的比较如表 3-2 所示。

表 3-2 定性、定量的风险评估方法比较

名称	定性评估方法	定量评估方法	定量与定性结合方法
定义	主要依据研究者的知识、经验、历史教训、政策走向及特殊案例等非量化资料对系统风险状况做出判断的过程	运用数量指标来对风险进行评估	定量分析是基础和前提;定性分析是灵魂,是形成概念、观点,做出判断,得出结论所必须依靠的
优点	可以挖掘出一些蕴藏很深的思想,使评估的结论更全面、更深刻;便于企业管理、业务和技术人员更好地参与分析工作,大大提高分析结果的适用性和可接受性	能够通过投资收益计算的客观结果来说服企业管理人员来推动风险管理;随着组织建立数据的历史记录并获得经验,其精确度将随着时间的推移而提高	在复杂的信息系统风险评估过程中,将这两种方法融合起来,取其优点
缺点	主观性很强,对评估者本身的要求很高;缺乏客观数据支持	计算过程复杂、耗时,需要专业工具支持和一定的专业知识基础;计算结果量化以后用财务术语描述有可能被误解和曲解	难度大,复杂度高

3.2.4 风险评估实施流程概述

要对一个复杂的信息系统进行正确的评估,并使得这个过程更有效率、更具可操作性,一个科学、合理的评估流程必不可少。图 3-3 给出了一个比较通用的评估实施流程。

风险评估准备:组织评估信息系统的安全性是一种战略性的考虑。评估前充分的准备能保证整个风险评估过程的有效性。

风险因素识别:包括资产识别、威胁识别和脆弱性识别、现有安全控制措施确认。通过前期准备阶段收集到的信息,将划入范围和边界的资产进行确认评估,并根据资产目前所处的环境条件和以前的报告记录情况来识别每项资产可能面临的威胁,对每一项需要保护的信息资产,找到可能被威胁利用的脆弱点并对其进行评估。现有的安全控制措施也是威胁事件发生的决定因素之一,因此也需要确认。

风险分析管理:依据前面对资产、威胁、脆弱性以及现有安全风险控制措施的识别结

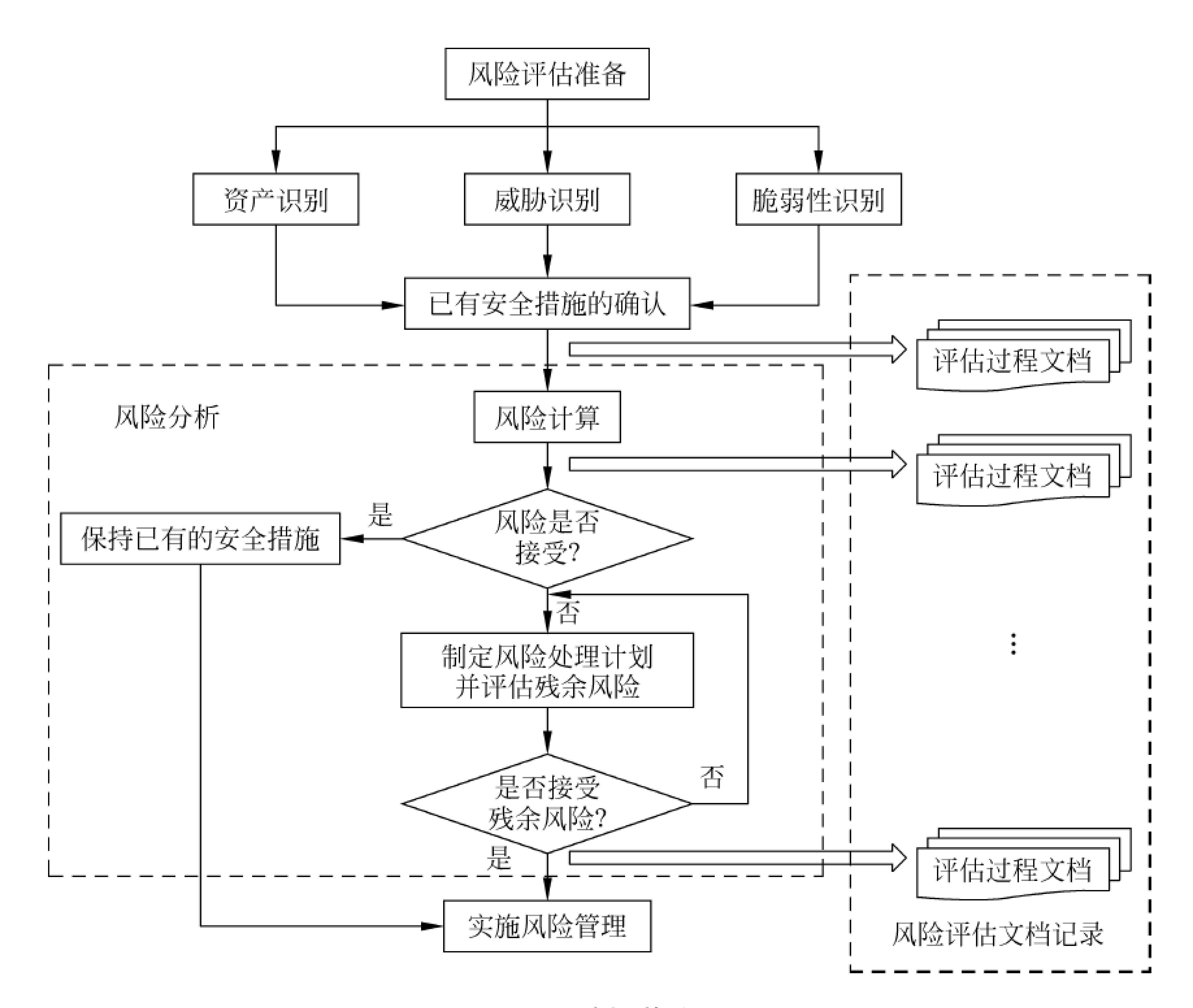


图 3-3 风险评估流程图

果,通过给定的风险计算模型进行风险计算,确定出各种风险所处的安全等级,并针对高风险区域给出风险控制方案。没有绝对的安全,风险评估的最终目的是使信息系统的安全风险降低到用户和决策者能够接受的程度。

风险评估文档记录:在项目进展过程中,风险评估的方法和结果都可能发生变化,所以详尽而完整的文档和材料非常重要。

信息系统的风险评估管理是一个不断降低风险的过程,可能需要进行多次评估。每次可根据条件和目的的不同,对这些步骤进行适当的调整。

3.3 风险评估相关标准

3.3.1 国外信息安全风险评估相关标准

1. OCTAVE

1) OCTAVE 简介

OCTAVE(Operationally Critical Threat,Asset and Vulnerability Evaluation,可操作的关键威胁、资产和弱点评估)是由美国卡耐基·梅隆大学软件工程研究所下属的 CERT 协调中心开发的一种信息安全风险评估的方法。这是一种信息安全风险评估规范,是从组织的角度开发的一种信息安全保护方法。

OCTAVE 信息安全风险评估方法，由一系列循序渐进的讨论会组成，每个讨论会都需要其参与者之间的交流和沟通。其核心是自主原则，即由组织内部的人员管理和指导该组织的信息安全风险评估。信息安全是组织内每个成员的职责，而不只是 IT 部门的职责。组织内部的人员需要负责信息安全评估活动，并对改进信息安全的工作做出决策。

OCTAVE 使组织能够理清复杂的组织问题和技术问题，了解安全问题，改善组织的安全状况并解决信息安全风险，而无须过分依赖外部专家和厂商。OCTAVE 包括两种具体方法：面向大型组织的 OCTAVE Method 和面向小型组织的 OCTAVE-S。

2) OCTAVE Method

OCTAVE Method 是为有 300 名以上员工的大型组织而设计的，但可以以此为基线或起点，对该方法进行开发剪裁，使它适合于不同规模的组织、业务环境或工业部门。

OCTAVE Method 包括三个阶段 8 个过程。

第 1 阶段：建立基于资产的威胁配置文件

这是从组织的角度进行评估，这一阶段的目标是建立组织对信息安全问题的概括认识。要实现这一目标，首先需要采集组织内员工对安全问题的个人观点，然后对这些个人观点进行综合整理，为评估过程中的所有后续分析活动提供依据。通过对组织专业领域知识的调研，可以清楚地表明员工对信息资产、资产面临的威胁、资产的安全需求、组织现行保护信息资产的措施等有关问题的理解。本阶段主要由 4 个过程组成。

(1) 过程 1：收集高层管理部门的观点，参与者为组织的高层管理人员。

(2) 过程 2：收集业务区域管理部门的观点，参与者为组织业务区域经理。

(3) 过程 3：收集员工的观点，参与者是组织的一般员工，信息技术部门的员工通常与一般的员工分开，参与一个独立的讨论会。

(4) 过程 4：建立威胁配置文件，包括整理过程 1～3 中所收集的信息、选择关键资产、提炼关键资产的安全需求、标志对关键资产构成影响的威胁等工作。

通用的配置文件是基于关键资产的威胁树。

第 2 阶段：识别基础设施的薄弱点

这一阶段也称为 OCTAVE Method 的“技术观点”。因为在这一阶段，分析人员的注意力转移到组织的计算基础设施上。在这一阶段中，对当前信息基础设施的评价包括数据收集和分析活动。通过检查信息技术基础结构的核心运行组件，可以发现导致非授权行为的漏洞或技术脆弱性。本阶段主要由两个过程组成。

(1) 过程 5：识别关键单元，包括识别结构单元的种类、要分析的基础设施的结构单元等。

(2) 过程 6：评估选定的单元，包括对选定的基础设施的结构单元进行薄弱点检查、对技术薄弱点进行评审并总结。

第 3 阶段：开发安全策略和计划

第 3 阶段旨在理解迄今为止在评估过程中收集到的信息，即分析风险。在这一阶段中，需要开发出解决组织内部存在的风险和问题的安全策略和计划。通过分析阶段 1 和阶段 2 中对组织和信息基础结构评估中得到的信息，可以识别出组织面临的风险，同时基于这些风险可能给组织带来的不良影响对其进行评估。此外，还要按照风险的优先级顺序制定出组织保护策略和风险缓解计划。本阶段主要由两个过程组成。

(1) 过程 7：执行风险分析，包括识别关键资产的威胁、制定风险评估标准、评估关键资产的威胁所产生的影响等。

(2) 过程 8：开发保护策略，评估小组开发整个组织的保护策略，该策略注重提高组织的安全实践，以及关键资产的重要风险的削减计划。

OCTAVE 的关键结果包括组织改进其安全状态的保护策略和减少组织关键资产风险的缓和计划。然而，评估结果仅为组织改进安全状态指明了方向，但不一定有重大改进。为了有效地管理信息安全风险，必须根据风险评估的结果开发详细的行动计划，并对这些计划的实施进行管理。

3) OCTAVE-S

OCTAVE-S 即 OCTAVE 简化版，是为规模较小的组织而开发的，这里将 20～80 名员工的组织视为小规模的组织。通过这种方法，3～5 人的评估小组就可以完成整个评估活动。与 OCTAVE Method 一样，OCTAVE-S 评估方法同样包括三个阶段，但其中的过程有些不同。

第 1 阶段：建立资产的威胁描述文件

本阶段主要由两个过程组成。

(1) 过程 S1：收集组织信息。分析小组应识别与组织重要信息相关的资产，确定一组评估标准，并定义组织当前的安全实践状况。

(2) 过程 S2：建立威胁描述。分析小组应选择 3～5 个关键信息资产，并为每个关键信息资产定义相应的安全要求和威胁描述文件。

第 2 阶段：识别基础设施的薄弱点

本阶段主要由一个过程组成。

过程 S3：检查与关键信息资产相关的计算基础设施。分析小组对关键资产支持系统中的访问路径进行分析，并确定这些技术措施对关键资产的保护程度。

第 3 阶段：开发安全策略和计划

本阶段主要由两个过程组成。

(1) 过程 S4：确定和分析风险。分析小组就风险所产生的影响、发生的可能性进行评估。

(2) 过程 S5：开发保护策略和风险降低计划。评估小组根据实际情况，开发一个整个组织范围的保护策略和风险削减计划。

2. SSE-CMM

1) SSE-CMM 概述

SSE-CMM 是 System Security Engineering Capability Maturity Model（系统安全工程能力成熟度模型）的缩写，它源于 CMM（能力成熟度模型）的思想和方法，是 CMM 在系统安全工程领域的应用，SSE-CMM 是偏向于对组织的系统安全工程能力的评估标准。

SSE-CMM 模型将信息系统安全工程分为三个相互联系的部分：风险评估、工程实施和可信度评估。针对这三个部分 SSE-CMM 定义了 11 项关键过程，并为每个过程定义了一组完成该过程必不可少的、确定的基本实践。同时模型还定义了 5 个能力成熟度等级，每个等级的判定反映为一组共同特性，而每个共同特性进而通过一组确定的通用实践来描述，通

用实践是对所有过程通用的工程实践。只有某一级别的所有共同特性都得到满足时，该过程的实施能力才达到对应的能力级别。

从整体上看，SSE-CMM 模型定义了一个"二维"架构，横轴上是 11 个系统安全工程的过程域，纵轴上是 5 个能力成熟度等级，如果给每个过程域赋予一个能力成熟度等级的评定，所得到的"二维"图形便形象地反映了安全工程的质量以及工程在安全上的可信度，也间接地反映了工程队伍实施安全系统工程的能力成熟性。

2）安全工程过程

（1）风险过程

风险是潜在的威胁、利用有用资源的脆弱性造成资源的破坏和损失。风险事件有三个组成部分：威胁、系统脆弱性、事件造成的影响。

安全机制在系统中存在的根本目的是将风险控制在可接受的程度内，SSE-CMM 模型定义了 4 种风险过程：评估威胁过程（PA04）、评估脆弱性过程（PA05）、评估风险事件影响过程（PA02），以及在前三种过程基础上的评估安全风险过程（PA03）。

（2）工程过程

安全工程是一个包括概念、设计、实现、测试、部署、运行、维护、废弃的完整过程。针对工程实施管理，SSE-CMM 模型定义了安全需求说明过程（PA10）、安全方案制定过程（PA09）、安全控制实施过程（PA01）、安全状态监测过程（PA08）。安全工程不是一个独立的实体，而是整个信息系统工程的一个组成部分，模型强调系统安全工程与其他工程的合作和协调，并定义了专门的协调安全过程（PA07）。

（3）保证过程

保证是指安全需求得到满足的信任程度。用可信度描述对建立的安全系统正确执行其安全功能的信心究竟有多大信任程度。传统方法是面向最终系统的方法，通过对系统所有文档和产品的严格分析和测试来建立可信度指标。但这种测试结果缺少继承性，当前工程的安全可信度与同一实施队伍依照类似工程过程在此之前所完成的工程的安全可信度并无直接关系，对每个工程的评测都要从头做起，于是导致了测试过程的复杂和冗长。SSE-CMM 模型在信任度问题上强调对安全工程结果可重复性的信任程度，它通过对现有系统安全体系真实性和有效性的测试（PA11）来构造系统安全可信度论据（PA06）。

3）能力成熟度等级

SSE-CMM 模型定义了 5 个能力级别。

1 级：非正式执行的过程。仅仅要求一个过程域的所有基本实践都被执行，而对执行的结果并无明确要求。

2 级：计划并跟踪的过程。这一级强调过程执行前的计划和执行中的检查。这使工程组织可以基于最终结果的质量来管理其实践活动。

3 级：完善定义的过程。过程域的所有基本实践均应依照一组完善定义的操作规范来进行。这组规范是实施队伍根据以往经验制定出来的，其合理性是验证过的。

4 级：定量控制的过程。能够对实施队伍的表现进行定量的度量和预测。过程管理成为客观的和准确的实践活动。

5 级：持续改善的过程。为过程行为的高效和实用建立定量的目标。可以准确地度量过程的持续改善所收到的效益。

3. GAO/AIMD

1998 年 5 月，美国审计总署(GAO)出版了《信息安全管理指南——向先进公司学习》(GAO/AIMD-98-68)，并出版了其支持性文件《信息安全风险评估指南——向先进公司学习》(GAO/AIMD-99-139)，GAO/AIMD-99-139 风险评估指南有针对性地对风险评估过程进行了分析和阐述，是在开展类似公司风险评估工作的过程中可以参考和借鉴的标准。

1) GAO/AIMD-99-139 的组成

GAO/AIMD-99-139 由三个部分组成：

第 1 部分是引言，介绍了风险评估指南的产生背景、风险评估在风险管理中的地位、风险评估过程的基本要素，以及信息安全风险评估过程中的难点。

第 2 部分给出了第 3 部分案例研究的概述，分析了风险评估过程中关键的成功因素、风险评估工具，以及风险评估带来的益处。

第 3 部分案例分析，美国审计总署从调查的众多组织中挑选了有代表性的 4 个组织，对他们的风险评估过程进行了分析和阐述。

GAO/AIMD-99-139 风险评估指南给出了风险评估指南的目标和方法论。

2) 风险评估过程的基本要素

风险评估过程通常要包括下列要素：

(1) 识别可能危害关键运作和资产并对其造成负面影响的威胁。

(2) 在历史信息及有经验人员判断的基础上，估计此类威胁发生的现实可能性。

(3) 识别并评价可能受到此类威胁发生影响的运作和资产的价值、敏感度和关键度，以确定哪些运作和资产是重要的。

(4) 对最关键、最敏感的运作和资产，估计威胁发生可能造成的潜在损失或破坏，包括恢复成本。

(5) 识别经济有效的措施以减轻或降低风险。

(6) 将结果形成文件并建立活动计划。

4. TCSEC

1985 年，美国颁布了可信计算机系统评估标准(Trusted Computer System Evaluation Criteria，TCSEC)，该标准为计算机安全产品的评测提供了测试内容和方法，指导信息安全产品的制造和应用，通常称为信息安全橘皮书。它将安全分为 4 个方面(安全政策、可说明性、安全保障和文档)和 7 个安全级别(从低到高依次为 D、C1、C2、B1、B2、B3 和 A 级)。

5. ISO/IEC 15408(CC)

信息安全产品和系统安全性测评标准，是信息安全标准体系中非常重要的一个分支，这个分支的发展已经有很长历史了，期间经历了多个阶段，先后涌现了一系列的重要标准，包括 TCSEC、ITSEC、CTCPEC 等，而信息产品通用测评准则(Common Criteria，CC)则是最终的集大成者，是目前国际上最通行的信息技术产品及系统安全性评估准则，也是信息技术

安全性评估结果国际互认的基础。

CC 的发展经历了一个漫长而复杂的过程，如图 3-4 所示。

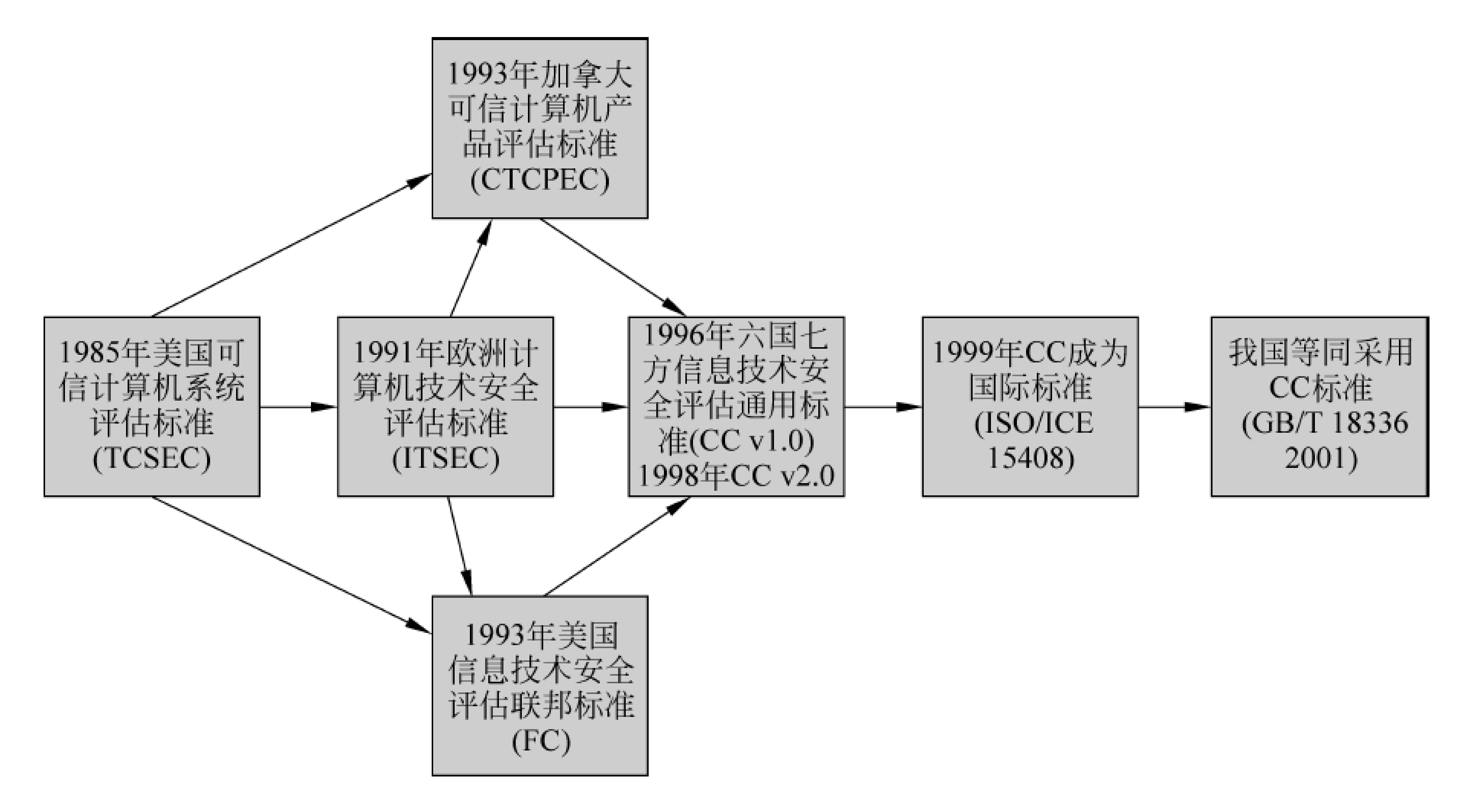


图 3-4 CC 的发展过程

从图 3-4 可以看出，CC 是由 TCSEC 等标准发展而来的；CC、ISO/IEC 15408 和 GB/T 18336 实际上是同一类标准，只不过 CC 是最早的称谓，ISO/IEC 15408 是正式的 ISO 标准，GB/T 18336 则是我国等同采用 ISO/IEC 15408 之后的国标。

CC 定义了评估信息技术产品和系统安全性所需的基础准则，是度量信息技术安全性的基准。它针对在安全评估过程中信息技术产品和系统的安全功能及相应的保证措施提出了一组通用要求，使各种相对独立的安全评估结果具有可比性，这有助于信息技术产品和系统的开发者或者用户确定产品或系统对其应用是否足够安全，以及在使用中存在的安全风险是否可以容忍。

CC 的主要目标读者是用户、开发者和评估者。CC 标准由三个文件构成，如表 3-3 所示。

表 3-3 CC 标准组成

代号	名　　称	简　　介
ISO/IEC 15408-1	Introduction and general model	介绍和一般模型。该部分定义了 IT 安全评估的基本概念和原理，提出了评估的通用模型
ISO/IEC 15408-2	Security functional requirements	安全功能要求。该部分按照“类-子类-组件”的方式提出了安全功能要求
ISO/IEC 15408-3	Security assurance requirements	安全保证要求。该部分定义了评估保证级别，介绍了“保护轮廓”和“安全目标”的评估，提出了安全保证要求

通过依据某个标准的风险评估或者得到该标准的评估认证，不但可为信息系统提供可靠的安全服务，而且可以树立单位的信息安全形象，提高单位的综合竞争力。

6. NIST SP800-30

NIST SP800-30 是由美国国家标准和技术学会(The National Institute of Standards and Technology,NIST)颁布的"信息技术系统风险管理指南",提供了把风险减少到一个可接受水平的非强制性指导原则,这个指南为开发一个有效的风险管理程序奠定了基础,包括一些定义和评估与减少 IT 系统内的风险所需的实用指南。

风险管理对一个组织通过以有效方式保护和管理 IT 资源来完成其使命非常重要。风险管理也支持信息系统的认证和鉴定。

在风险管理中担任一定角色的关键人员如下:高级管理者、首席信息官(Chief Information Officer,CIO)、系统和信息的所有者、商业和部门经理、信息系统安全官员(Information System Security Officer,ISSO)、IT 安全从业人员、安全意识培训师。

NIST SP800-30 将风险定义为既定威胁源利用特定潜在漏洞的可能性和该负面事件对组织造成的影响的函数。

NIST SP800-30 定义风险管理具有以下三种成分:风险评估、风险缓解、风险评价。

风险评估包括以下步骤:系统表征、威胁识别、漏洞识别、控制分析、可能性判断、影响分析、风险确定、控制建议、结果文档。

风险缓解优先考虑从风险评估活动中得出的被推荐的控制措施。要对控制措施进行成本效益分析,以把风险限制到完成组织任务所需的一个可接受的水平。为了缓解风险,可以运用技术、管理和操作控制。风险缓解包括以下方面:风险规避、风险承担、风险限制、风险转移、风险规划和研发。

一个组织经常会经历人事、网络体系结构和信息系统的变动,因此风险管理是一个连续过程,需要不断进行评价和评估。

3.3.2 国内信息安全风险评估相关标准

1. GB/T 20984—2007 信息安全技术 信息安全风险评估规范

本标准提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法,以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。本标准适用于规范组织开展的风险评估工作。

随着我国信息化应用的逐步深入,信息安全问题也日益受到关注,针对我国没有信息安全风险评估标准的现状,2004 年,国信办组织专家启动信息安全风险评估的研究与标准的编制工作,标准编制工作于 2004 年 3 月正式启动,2007 年 7 月通过了国家标准化管理委员会的审查批准,标准编号和名称为 GB/T 20984—2007《信息安全技术 信息安全风险评估规范》,于 2007 年 11 月正式实施。

GB/T 20984—2007《信息安全技术 信息安全风险评估规范》包括正文和附录两部分,正文由前言、引言和 7 章内容组成,附录部分包括附录 A 和附录 B,均为资料性附录。

前言:对本标准的制定作了简单介绍。

引言:简单介绍了信息安全风险评估的重要性。

第 1 章 范围:阐述了本标准的范围。

第 2 章　规范性引用文件：阐述了本标准的规范性引用文件。

第 3 章　术语和定义：给出了信息安全风险评估中涉及的术语和它们的定义。

第 4 章　风险评估框架及流程：阐述了信息安全风险评估中各要素的关系、风险分析的原理、风险评估的实施流程。

第 5 章　风险评估实施：详细介绍了信息安全风险评估的实施过程及每一阶段的具体任务和职能。

第 6 章　信息系统生命周期各阶段的风险评估：阐述了信息安全风险评估在信息系统生命周期各阶段中的不同要求。

第 7 章　风险评估的工作方式：介绍了风险评估的两种形式、自评估和检查评估。

附录 A 风险的计算方法：详细介绍了目前比较常用的两种风险计算方法，即矩阵法和相乘法。

附录 B 风险评估工具：对当前的风险评估工具进行了分类和综述。

2. 其他标准

GB/T 18336—2001《信息技术　安全技术　信息技术安全性评估准则》是 2001 年参照国际标准 ISO/IEC 15408：1999，我国制定的在信息安全技术方面的第一个国家标准，作为评估信息技术产品与信息安全特性的基础准则。GB/Z24364—2009 是信息安全风险管理指南。

3.4　风险评估工具

风险评估工具是一种辅助性的手段，通过对某一个系统对象的自动化或半自动化的分析，反映出系统主要部件的客观状况。评估工具还能够将专家知识进行集中，通过专家知识的应用，在风险评估中发挥重要的辅助作用。根据工具应用的目标和在风险评估中的工作方式，可将风险评估工具分为：主动型评估工具、被动型评估工具、管理型评估工具三种类型。

主动型评估工具是基于某种固定的“询问—回答”模式，将某些人工指令操作集成在一起自动执行。“询问—回答”方式是建立在大量设备知识或协议知识基础上的，如通过对服务器某个端口的询问，并分析设备的返回结果而得到关于该设备端口状况的结论。主动型评估工具集成的知识可以弥补评估人员知识面的不足。各类扫描器是典型的主动型评估工具，如 Tenable Nessus、X-Scan、AppDetective、ISS DBScanner、Metasploit Framework 等。被动型评估工具是一种立足于“防御”的角度收集系统信息并进行简单分析的工具。最典型的被动型评估工具如入侵检测产品、网络监控流量分析产品、主机完整性检测产品等。与主动型评估工具不同，被动型评估工具并不主动“询问”评估对象，而是采用被动方式捕获目标信息系统数据，收集评估所需要的数据和资料，发现存在的薄弱点，帮助完成现状分析和趋势分析。目前比较常用的被动型评估工具有：SnifferPro、Wildpackets Etherpeek NX、Fluke DSP4000 等。管理型评估工具可以直接使用主动型评估工具的评估结果，甚至可以将主动型、被动型评估工具集成在系统中。目前比较常用的管理型评估工具有 CRAMM、COBRA、IAS 等。表 3-4 给出了几种典型的风险评估与管理工具的比较分析。

表 3-4 综合风险评估与管理工具的比较

工具名称	COBRA	RA	CRAMM	@RISK	BDSS
组织/国家	BSI/Britain	BSI/Britain	CCTA/Britain	Palisade/America	The Integrated Risk Management Group/American
体系结构	客户-服务器	单机版	单机版	单机版	单机版
采用方法	专家系统	过程式算法	过程式算法	专家系统	专家系统
定性/定量算法	定性/定量结合	定性/定量结合	定性/定量结合	定性/定量结合	定性/定量结合
数据采集形式	调查问卷	过程	过程	调查文件	调查问卷
对使用人员的要求	不需要有风险评估的专业知识	依靠评估人员的知识与经验	依靠评估人员的知识与经验	不需要有风险评估的专业知识	不需要有风险评估的专业知识
结果输出形式	风险等级与控制措施	风险等级与控制措施	风险等级与控制措施	决策支持信息	安全防护措施列表

思考题

1. 简单叙述风险评估依据的主要内容。
2. 简单叙述风险评估原则的主要内容。
3. 解释风险要素关系模型。
4. 叙述风险分析原理。
5. 论述风险评估方法。
6. 叙述风险评估实施流程。
7. 查阅资料，归纳国内外信息安全风险评估相关标准。

第4章 IT治理概述

4.1 IT 治理

企业信息化建设的根本是实现企业战略目标和信息系统整体部署的有机结合。企业信息技术的管理工作一般可以分为三层架构,IT 战略规划层(战略层)、IT 系统管理层(战术层)和 IT 技术及运作管理层(运作层)。其中,IT 战略规划内容包括 IT 战略制定、IT 治理和 IT 投资管理;IT 系统管理内容包括 IT 管理流程、组织设计、管理制度和管理工具等;IT 技术及运作管理内容包括 IT 技术管理、服务支持和日常维护等。

IT 治理是组织根据自身文化和信息化水平构建适合组织发展的架构并实施的一种管理过程,是平衡 IT 资源和组织利益相关者之间 IT 决策权力归属与责任分配的一种管理模式,旨在规避 IT 风险和增加 IT 收益,实现 IT 目标与组织业务目标的融合。

IT 治理是信息技术、经济学及管理学界中的一个概念,用于描述企业或政府是否采用有效的机制,使得 IT 的应用能够完成组织赋予它的使命,同时平衡信息化过程中的风险,确保实现组织的战略目标。其主要使命是:保持 IT 与业务目标一致,推动业务发展,促使收益最大化,合理利用 IT 资源,适当管理与 IT 相关的风险。

IT 治理的目的之一就是通过平衡信息技术和信息过程的风险,使得 IT 能够实现其预期的功能,并帮助企业实现其战略目标,改善企业经营的业绩,从而增加企业的收益与核心竞争力。针对信息系统的风险控制是顺利实现 IT 治理的必要过程,主要包括信息系统风险的识别、量化评估以及采取什么样的措施来规避风险。

IT 战略目标必须与企业战略目标保持一致,IT 对于组织来说非常关键,是战略规划的重要组成部分,甚至直接影响到战略竞争机遇。具体内容如下:

(1) IT 治理包含治理委员会、治理结构、治理流程和企业文化等。

(2) IT 治理使风险透明化,从而保护利益相关者的权益。

(3) IT 治理可用来指导和控制 IT 投资、机遇、收益及风险。

(4) IT 治理通过引导 IT 战略,并建立标准的信息基础架构,实现业务增长。

(5) IT 治理对核心 IT 资源做出合理的制度安排,这将成为进入新的市场、进行有效竞争、实现总收入增长、改善客户满意度及维系客户关系的制度保障。

虽然 IT 治理的定义不同,但在 IT 治理研究领域中,有一些本质的东西是被广泛认可的。例如,IT 治理是企业治理的组成部分;IT 治理解决的是做什么和由谁负责的问题;IT 治理的目标是实现和促进企业目标等。与业务目标一致、有效利用信息资源和风险管理是

实施IT治理的本质。

IT治理是一个循环反复的过程，包括IT的规划与实施、IT及信息的获取与实施、信息系统的交付与支持、过程的监控等，在管理IT风险的同时实现收益，通过回顾评估进行修正，然后进入下一个循环。

公司治理的重点是注重战略目标的制定，注重创新能力的鼓励和保障，侧重于客户以及利益相关者的关系；IT治理的侧重点是关注与目标相匹配的过程实现，注重在有效的机制下对知识资产和智力资产进行管理和关注企业之间的沟通和内部成员之间的沟通。

4.2 IT治理支持手段

目前国际上较为通行公认的IT治理标准主要有：COBIT、PRINCE2、ITIL、ISO/IEC27001以及COSO发布的内部控制框架等。COBIT提供控制和审计；PRINCE2提供结构化项目管理方法；ITIL提供整个过程的服务管理；ISO/IEC27001提供安全管理。除此之外，CISR强调决策权的分配；IT-CMM可以判定企业信息化级别。

1. 内部控制理论与ERMF

20世纪90年代初，美国COSO委员会(Committee of Sponsoring Organizations of the Treadway Commission，全美反舞弊性财务报告委员会发起组织)在整合企业对内部控制需求的基础上提交报告《内部控制——整体框架》。两年后，COSO对整体框架进行了更全面的增补，随后此框架得到了众多企业的认可，并于4年后获得了美国《审计准则公告第78号》的承认。而且COSO内部控制框架还得到美国证券交易委员会的信赖，由此可见该框架在当时的作用是非常明显的。COSO内部控制整体框架认为：内部控制系统是由控制环境、风险评估、内控活动、信息与沟通、监督5个要素组成。该框架强调内部控制与管理是一个过程。不同的企业对信息系统进行风险控制时，5个要素的内容可能各不相同，这与企业管理层选择的经营方式有关。2004年，COSO报告对内部控制整体框架进行了改进，提出了企业风险管理(Enterprise Risk Management，ERM)的概念，成为内部控制研究道路上一个新的里程碑。此报告将原来内部控制的3大目标增加到4个，并基于内部控制和企业风险管理的新需求，将5大要素扩展到8个。该报告还首次将风险评估作为内部控制的组成部分，使得内部控制的理论更加完善。COSO对企业风险管理的定义中明确指出，企业风险管理是一个企业全体人员共同参与的过程，它包括内部控制及其在战略和整个组织的应用，旨在为实现企业经营目标和企业正常运行规范提供合理保证。COSO认为风险管理是由目标、要素和组织三个维度组成的整体框架，ERMF(Enterprise Risk Management Framework)框架结构如图4-1所示。

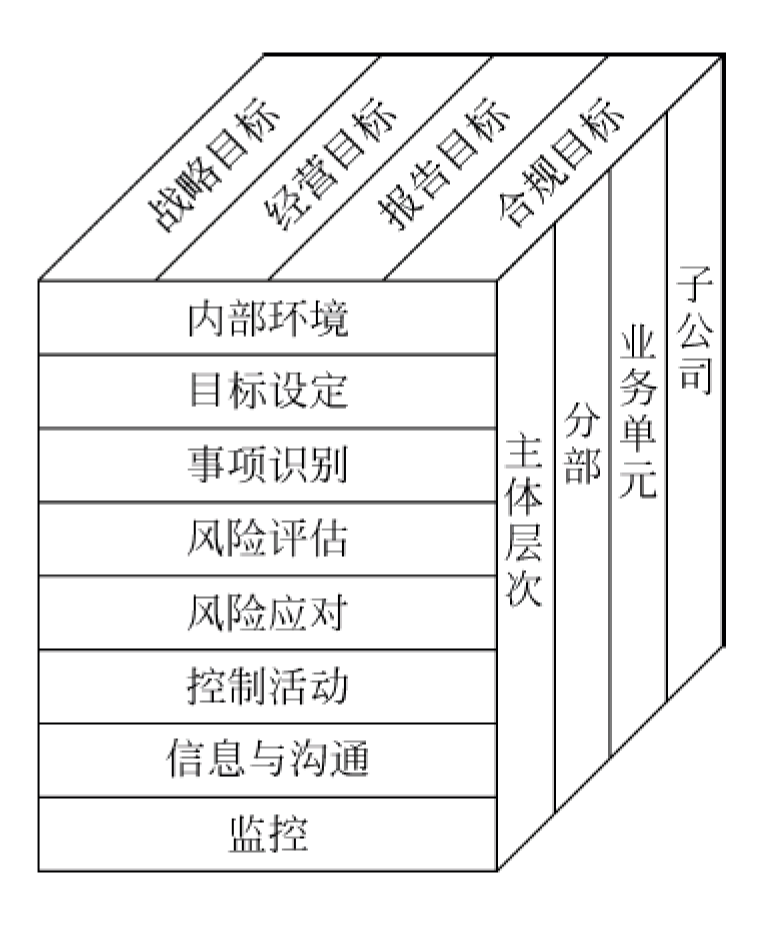


图4-1 ERMF框架

第一维度、企业的目标：主要包括战略目标、运营目标、报告目标和合规目标等，这些目标为企业的运营起到

了方向性的指导作用。

第二维度、企业风险管理要素：内部环境、目标设定、事项识别、风险评估、风险应对、控制活动、信息与沟通和监控，这些要素是企业进行风险控制的主要考虑对象。

第三维度、企业的组织结构，也就是公司从上至下的组织层次结构，主要包括主体层次、分部、业务单元及子公司等。

2. PRINCE2

1975 年，Simpact Systems 公司建立项目管理方法 PROMPT；1979 年，英国 CCTA (Central Computer and Telecommunications Agency，中央计算机与电信局)将 PROMPT 接受为政府部门信息系统项目的项目管理标准；1989 年，PRINCE(PRojects IN Controlled Environments，受控环境中的项目)取代了 PROMPT；1996 年，CCTA 并入英国政府商务部(OGC)对 PRINCE 做了进一步的开发，形成 PRINCE2，并开始推广。

项目管理向来就是一个充满挑战的管理，管理人员必须在事先确定好的人力、物力、财力和时间基础上产出预期质量的项目结果。PRINCE2 是结构化的项目管理方法，其过程模型由 8 个管理过程组成，这 8 个过程涵盖了从项目启动到结束过程中进行项目管理和控制的所有活动。每个过程都鼓励对项目责任正式的确认，强调项目交付什么、为何交付、交付时间和为谁交付。

在 PRINCE2 框架指导下，其 8 个管理过程在每一个具体项目中必须以合适的方式定义和完成，它们是 PRINCE2 实施步骤的指导，而 PRINCE2 所定义的 8 个管理要素，其方法理念将在过程的实施中得以体现。这 8 个要素分别如下。

(1) 商业论证。PRINCE2 的首要前提就是必须有可操作的商业论证来驱动项目的运作。只有当商业论证有变化需求时，项目过程中的各种基础特征才能清晰定义与管理。

(2) 组织。PRINCE2 提供了项目管理团队的组织构架，定义了项目相关人员的角色、责任以及关系。其中，有部分角色可以根据项目实际情况进行适当的合并或者分担。

(3) 计划。PRINCE2 提供了一系列不同级别的计划模板以及基于成果的计划方法，以方便使用者根据项目大小与具体需求来量身定做自己的项目计划。

(4) 控制。PRINCE2 拥有一套控制机制以方便关键决策信息的提供，帮助项目组织避免问题出现以及更好地处理问题。PRINCE2 的高级管理控制是基于例外管理这一概念的。这就是说一旦计划得以批准，项目经理就应该将计划推行下去，直到可能发生问题之时。

(5) 风险管理。风险是 PRINCE2 贯穿于整个项目生命周期中所重点关注的因素。PRINCE2 定义了何时应该检查风险，提供了一套分析管理风险的方法，并要求在所有过程中施行。

(6) 项目环境质量。PRINCE2 认识到质量的重要性，在管理和技术过程中融入了质量方法。该方法包括设定用户质量期望，明晰质量标准以及实施质量检测方法。

(7) 配置管理。意为跟踪最终产品要素以及发行版本。配置管理的办法有很多，PRINCE2 并没有提出新的方法，而是说明了配置管理方法所需的基本要求以及它是怎么和其他要素、技术联系在一起的。

(8) 变更控制。PRINCE2 认为项目过程中所实施的技术手段会因为环境以及项目本

身的原因而发生很大的差异，因此，它没有推荐相应的实现工具和技术，而是一再强调具体实施技术和工具要根据具体情况确定，项目经理可以要求项目支持组提供相应的技术和工具。但是，PRINCE2 仍然描述了三项技术：基于产品的计划方法；质量审查技术；变更控制技术。

PRINCE2 提供一套控制手段，保证提供进行关键决策所需要的信息；PRINCE2 规定了风险审核关键点，同时概述了风险分析和管理方法；PRINCE2 在技术和管理过程中融入了质量方法；PRINCE2 对配置管理方法所需要的信息和基本设施进行了定义，也说明了应如何与 PRINCE2 的其他几个组成部分进行衔接；PRINCE2 强调变更控制的必要性。

3. ITIL

信息技术基础架构库(Information Technology Infrastructure Library，ITIL)由英国政府部门 CCTA(Central Computing and TelecommunicationsAgency)在 20 世纪 80 年代末制定，现由英国商务部 OGC(Office of Government Commerce)负责管理，主要适用于 IT 服务管理(ITSM)。ITIL 模型起源于 20 世纪 80 年代末，最初的目的是通过应用 IT 提升政府业务的效率。ITIL 开始是作为政府 IT 部门的最佳实践指南，之后被推广到英国私营企业，然后传遍欧洲，兴起于美国。20 世纪 90 年代后期，ITIL 的思想和方法，被美国、澳大利亚、南非等国家广泛引用，并进一步发展。2001 年，英国标准协会(British Standard Institute，BSI)在国际 IT 服务管理论坛(itSMF)年会上，正式发布了基于 ITIL 的英国国家标准 BS15000。2002 年，BS15000 为国际标准化组织(ISO)所接受，作为 IT 服务管理的国际标准的重要组成部分。ITSM 领域已经成为全球 IT 厂商、政府、企业和业界专家广泛参与的领域，对未来的 IT 走向和企业信息化，将会产生深远的影响。其内容描述的是 IT 部门应该包含的各个工作流程以及各个工作流程之间的相互关系。

ITIL 自 1980 年至今，主要经历了三个主要版本：ITIL v1(1986—1999)、ITIL v2(1999—2006)和 ITIL v3(2004—2007)。ITIL v1 是基于职能型的实践，有四十多卷图书；ITIL v2 是基于流程型的实践，有 10 本图书，包含 7 个体系。此时，已经成为 IT 服务管理领域全球广泛认可的最佳实践框架；ITIL v3 基于服务生命周期的实践，整合了 ITIL v1 和 ITIL v2 的精华，是 IT 服务管理领域当前的最佳实践。ITIL 已经成为 IT 管理领域的事实上标准，相关的 IT 产品有 IBM 的 Tivoli、微软公司的 MOF(Microsoft Operations Framework，微软运营框架)、惠普公司的 ITSM 参考模型(IT Service Management Reference Model)等。

1999 年，ITIL 引入中国。1999—2002 年，国内对 ITIL 了解的单位不多，成功案例也十分有限。2002 年开始日益受到关注。

ITIL 主要包括 6 个模块，即服务管理、业务管理、IT 服务管理规划与实施、基础架构管理、应用管理和安全管理。服务管理是 ITIL 中 6 个模块中的最核心模块，其又包括服务支持和服务提供。服务支持流程组包括 5 个运营级流程：事故管理、问题管理、配置管理、变更管理以及发布管理。服务提供流程组包括 5 个战术级流程：服务级别管理、IT 服务财务管理、能力管理、IT 服务持续性管理和可用性管理。

ITIL 的特点有：ITIL 作为最佳实践框架不是基于理论开发的，而是根据实践开发的；ITIL 是事实上的国际标准；ITIL 内含质量管理思想。ITIL 为企业的 IT 服务管理实践提供了一个客观、严谨、可量化的标准和规范。ITIL v3 拥有三个组件：核心组件、补充组件和

网络组件。核心组件由5本书组成,替代了原有的两本书"服务支持"和"服务交付",涵盖了IT服务的生命周期,从设计到退役,其包括关键概念和相对稳定、通用化的最佳实践。补充组件包括不同情况、行业和环境的详细内容和目标。ITIL v3新的特色是补充组件,该部分指导在不同市场、技术或规范环境中的应用。补充组件将每年或每季度不定期地根据需求进行变更。网络组件提供共同所需的动态资源和典型资料,例如流程图、定义、模板、业务案例和实例学习。网络组件是动态的在线资源,可根据需要进行变更,类似于一个公司的网站。

ITIL v3的核心架构是基于服务生命周期的。服务战略是生命周期运转的轴心;服务设计,服务转换和服务运营是实施阶段;服务改进则在于对服务的定位和基于战略目标对有关的进程和项目的优化改进。

ITIL自发布以来,一直被业界认为是IT服务管理领域事实上的管理标准,直到2000年11月,英国标准协会(BSI)正式发布了以ITIL为核心的国家标准BS15000;随后,2005年5月,国际标准组织(ISO)以快速通道的方式批准通过了ISO 20000的标准决议,并于同年12月15日正式发布了ISO 20000标准。

ISO/IEC 20000-1是由联合技术委员会ISO/IEC JTC1信息技术组发布的,其第2版取代了第1版(ISO/IEC 20000-1:2005),也进行了技术修订。其主要区别如下:更接近ISO 9001;更接近ISO/IEC 27001;对术语进行了调整,以保持和国际惯例的一致性;加入了更多的定义,对一些定义进行更新,对其中的两个定义进行清除;引进了"服务管理体系"的概念;将ISO/IEC20000-1:2005版中的条款3和条款4进行了合并,并将所有的管理体系要求纳入到同一个条款中;进一步明确了运营流程各方的治理要求;进一步明确了定义服务管理体系范围的要求;进一步明确了将PDCA方法应用于服务管理体系中,包括服务管理流程和服务;对新服务和变更服务的设计与转换引进了一些新的要求。

ISO 20000的流程包括ITIL v2中核心模块服务支持和服务提供的所有相关流程,以及安全管理和其他模块的相关流程。ITIL v3则在v2的基础上,参照ISO 20000的管理体系,进一步地明晰和增加了部分流程。ISO 20000包含13个管理流程。除了服务报告之外,ITIL v2囊括了ISO 20000中的所有管理流程,并增加了服务台这个流程,作为报告事件和请求提供用户支持的中心,作为首次联系点,对事件进行统计和归类,有效减轻了IT部门的工作量。ITIL v3是在ITIL v2的基础上发展起来的,它用生命周期的概念将ITIL v2中设计的各个管理流程有机地贯穿在了一起,以服务战略为指导,从服务设计开始,通过服务转换,直至服务运营,整个过程井然有序,同时伴随着持续服务改进,用以提高各个模块的服务水平。ITIL v3是用一种全新的视角对ISO 20000中的管理流程进行了整合,根据各个流程的特性及所处的阶段,将它们归纳到不同的服务生命周期过程中,如表4-1所示。

表4-1 ISO 20000、ITIL v2与ITIL v3流程

ISO 20000流程	ITIL v2流程	ITIL v3流程	所属v3生命周期阶段
事故管理	事故管理	事件管理、事故管理、请求实现	服务运营
问题管理	问题管理	问题管理	服务运营
变更管理	变更管理	变更管理	服务转换

续表

ISO 20000 流程	ITIL v2 流程	ITIL v3 流程	所属 v3 生命周期阶段
配置管理	配置管理	配置管理	服务转换
发布管理	发布管理	发布管理	服务转换
服务级别管理	服务级别管理	服务级别管理	服务设计
服务连续性 & 可用性管理	服务连续性管理 & 可用性管理	连续性管理 & 可用性管理	服务设计
IT 服务预算和会计	财务管理	IT 服务财务管理	服务战略
能力管理	能力管理	能力管理	服务设计
服务报告	(无)	服务报告	服务改进
信息安全管理	安全管理	信息安全管理	服务设计
业务关系管理	《业务管理》&《用户联络》	业务关系管理	服务战略
供应商管理	ITIL 丛书第一版 &《业务管理》	供应商管理	服务设计
(无)	(无)	知识管理	服务转换

4. COBIT 模型

COBIT(Control Objectives for Information and related Technology)是目前国际上通用的信息系统审计的标准,由 ISACA(The Information System Audit and Control Association,美国信息系统审计与控制协会)在 1996 年公布。这是一个在国际上公认的、权威的安全与信息技术管理和控制的标准,目前已经更新至 5.0 版。它在商业风险、控制需要和技术问题之间架起了一座桥梁,以满足管理的多方面需要。该标准体系已在世界一百多个国家的组织中运用,指导这些组织有效地利用信息资源,有效地管理与信息相关的风险。目前 COBIT 模型已经有 6 个版本,分别是 COBIT 1.0(1996),COBIT 2.0(1998),COBIT 3.0(2000),COBIT 4.0(2005),COBIT 4.1(2007),最新版本为 2012 年 4 月颁布的 COBIT 5.0。2012 年 4 月,ISACA 官方正式发布 COBIT 5.0,这是 COBIT 发展 16 年来最重大的一次变化。COBIT 5.0 通过整合其他重要框架对 COBIT 4.1 进行扩展而成。COBIT 5.0 提供了一个组织 IT 治理的端到端业务视图,该视图反映了信息技术在创造业务价值时的重要作用。该框架中提供了全球广泛认可的原则、最佳实践、分析工具和模型,可帮助组织获得对信息系统的信任并从中产生价值。

最初 COBIT 模型是用于 IT 审计的知识体系,着重用于 IT 的安全管理和风险控制,随后逐步发展成为 IT 治理的一整套体系标准。该标准为 IT 治理、安全与控制提供了一个结构化、系统化的框架,组织的各级人员基于这个框架展开 IT 治理。同时,COBIT 也是一个最佳实践库。COBIT 管理指南给出了 COBIT 的控制过程,COBIT 框架从信息系统的规划与组织、获得与实现、交付与支持、监控 4 个方面确定了通用的信息技术处理过程,只要通过对信息系统风险控制的过程进行评估,就可以帮助组织掌握信息系统外部环境。COBIT 为组织提供了过程框架在不同领域的良好实践,并以逻辑清晰且便于管理的架构来展示控制活动。

COBIT 5.0 提出了能使组织在一套包含 7 个驱动因素整体方法下、建立有效治理和管理框架的 5 个原则,以优化信息和技术的投资及使用以满足相关者的利益,如图 4-2 所示。

原则 1　满足利益相关者需求：组织存在的目的是为利益相关者创造价值，这些价值的创造通过保持效益、风险和资源使用优化之间的平衡来实现。COBIT 5.0 通过应用 IT 提供所有的必要的规程和促成因素来支持价值创造。因为不同组织有不同的目标，组织可以通过目标关联，自定义 COBIT 5.0 以适合其自身的情况，将高级别的组织目标转化成易管理、特定的、IT 相关的目标，并将它们映射到具体的流程与实践。

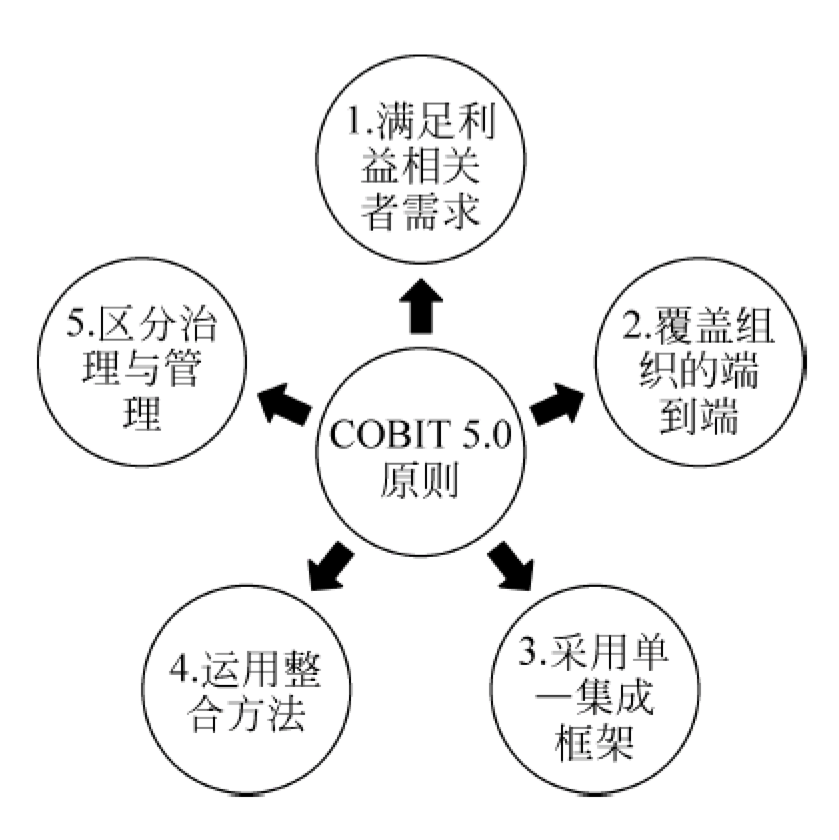


图 4-2　COBIT 5.0 原则

原则 2　覆盖组织的端到端：COBIT 5.0 将企业 IT 治理融合到企业治理中，包含组织内的所有职能部门与流程；COBIT 5.0 不仅关注 IT 部门，而且把信息与相关技术当作资产，就像公司中每个人拥有的其他资产一样；考虑到了所有端到端的和组织范围的 IT 相关的治理和管理的促成因素，也就是说，包括组织内部和外部的、与组织的信息和涉及的 IT 治理与管理相关的各种要素和人员。

原则 3　应用一个单一的集成框架：有许多 IT 相关标准和最佳实践，每一个均提供一部分 IT 活动的指导，COBIT 5.0 与其他相关标准与框架保持高度一致，并因此能够成为企业 IT 治理和管理的总体框架。

原则 4　运用了整合方法：有效的企业 IT 治理和管理，需要一种整体考虑多个组件间相互影响的方法，COBIT 5.0 定义一系列促成因素来支持企业 IT 综合治理和管理系统的实施。

原则 5　区分治理与管理：COBIT 5.0 关于管理与治理的区别的观点在于“治理是保证通过评估利益相关者的需求、条件和选择权，以决定所要实现的、平衡的、一致的组织目标，通过优先次序设定方向、进行决策，并监控绩效实体以及既定方向和目标的符合性；管理是规划、构建、运营和监控与治理机构所设定的方向保持一致的活动，以实现企业目标。”

COBIT 5.0 包含的 7 个驱动因素如图 4-3 所示。

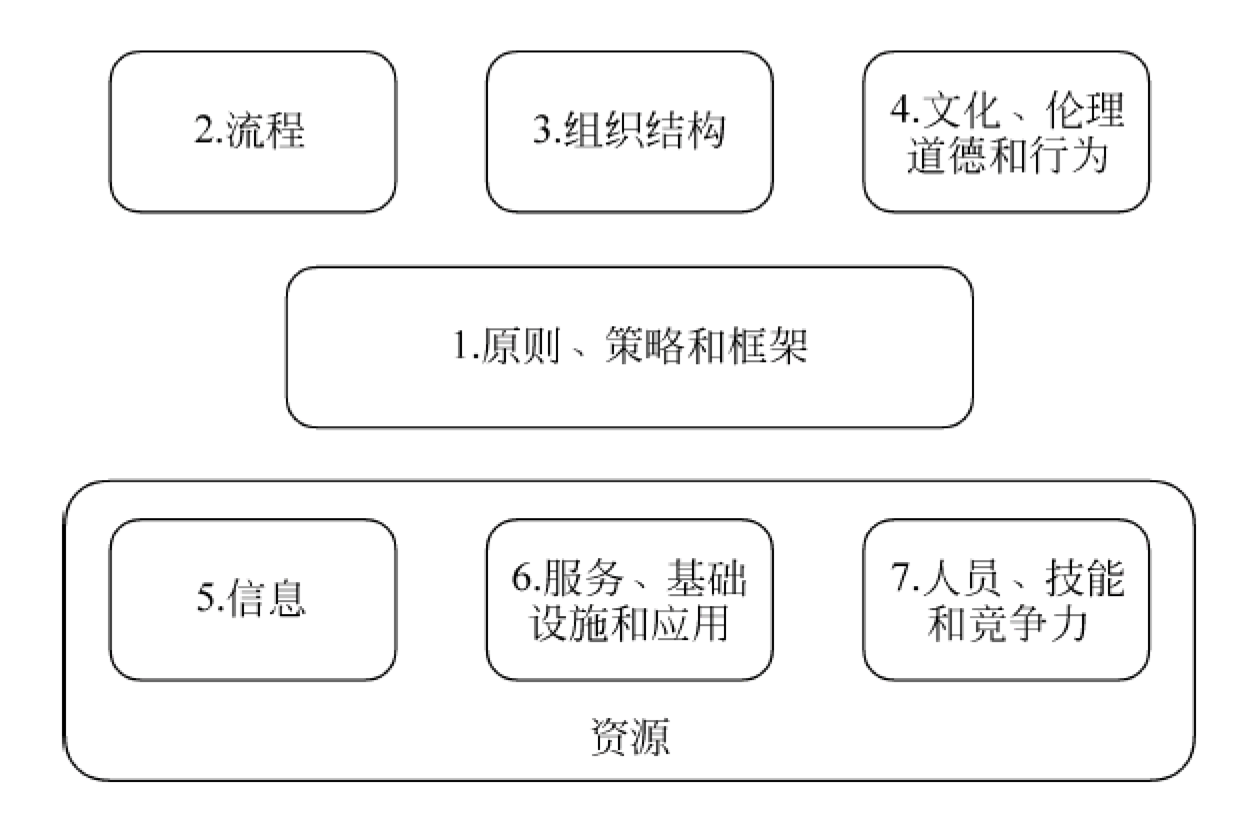


图 4-3　COBIT 5.0 企业促成因素

（1）“原则、策略和框架”是将期望的行为转化为实际指南的手段，以指导日常管理。

（2）“流程”描述了为实现既定目标的一系列有组织的实践和活动，同时产生支持实现全部 IT 相关目标的一系列结果。

（3）“组织结构”是企业中决策的关键实体。

（4）“文化、伦理道德和行为”是治理和管理活动中不可忽略的成功因素。

（5）“信息”是保持组织运营和良好治理所必需的要素，也是企业本身在操作层面的关键产品。

（6）“服务、基础设施和应用”系统，包括为组织提供信息技术处理和服务的基础架构、技术及应用系统。

（7）“人员、技能和竞争力”是成功完成所有活动，并做出正确选择及采取纠正措施所必需的要素。

COBIT 5.0 不是规定性的，但它主张组织实施治理和管理流程以涵盖关键领域，如图 4-4 所示。COBIT 5.0 流程参考模型将组织 IT 治理和管理流程分为两个主要流程领域：

（1）治理：包括 5 个治理流程，在每个流程内，定义了评估、指导和监控实践。

（2）管理：包含 4 个领域，责任区域的规划、构建、运行和监控，并提供 IT 端到端的覆盖。

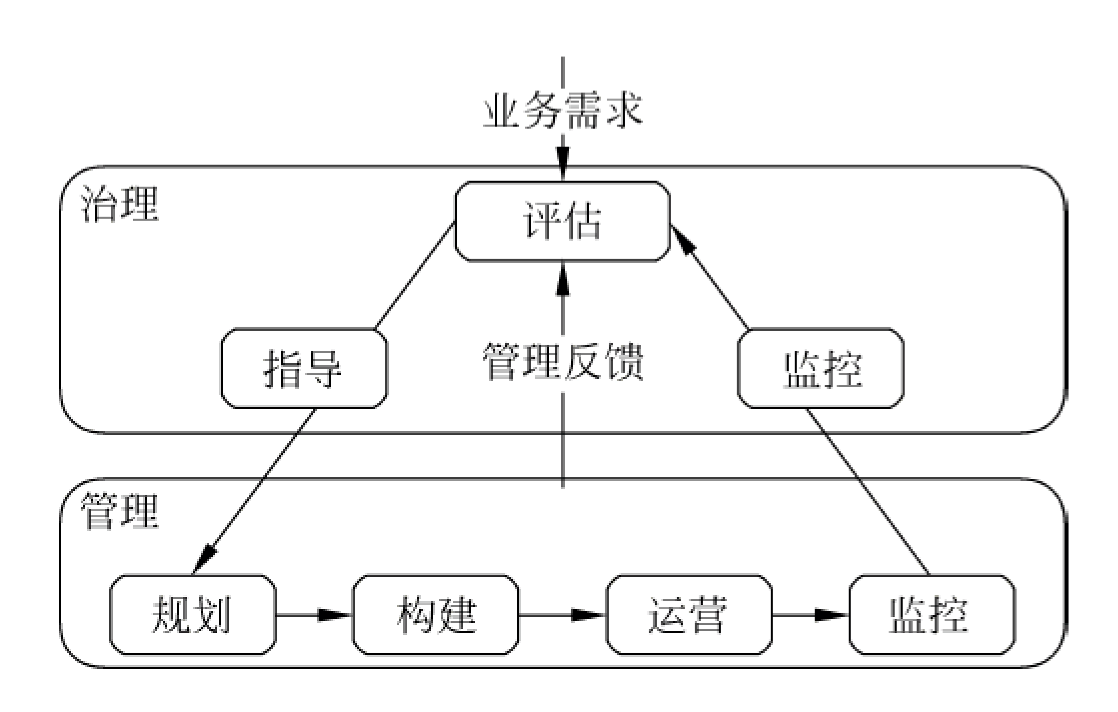


图 4-4　COBIT 5.0 治理与管理的关键领域

COBIT 5.0 流程参考模型是 COBIT 4.1 流程参考模型的继承者，同时也融合了 Value IT、Risk IT 流程模型。COBIT 5.0 包含 37 种治理和管理流程的集合。

ITIL v3 2011 和 ISO/IEC 20000 包括 COBIT 5.0 中的以下领域：DSS 领域流程子集、BAI 领域流程子集、APO 领域一些流程；ISO/IEC 27000 包括 COBIT 5.0 中的以下领域：EDM、APO 和 DSS 中安全和风险相关流程、其他领域流程各种安全相关活动、MEA 领域监控和评估活动；PRINCE2 包括 COBIT 5.0 中的以下领域：APO 域组合相关的流程、BAI 域的方案和项目管理流程。

表 4-2 给出了所有 COBIT 5.0 所涵盖的来自 COBIT 4.1 的信息，且 COBIT 5.0 的信息模型允许定义另一套标准，因此增加了 COBIT 4.1 标准的价值。

5. 标准间的相互关系

COBIT 基于已有的许多架构，如 SEI 的能力成熟度模型（CMM）对软件企业成熟度的 5 级划分，以及 ISO 9000 等标准，在总结这些标准的基础上重点关注企业需要什么，而不是

表 4-2　COBIT 5.0 与 COBIT 4.1 信息标准对等定义

COBIT 4.1 信息标准	COBIT 5.0 的对等定义
有效性	如果信息满足了为完成特定任务而使用、满足信息消费者的需求，那么它是有效的；如果信息消费者可以使用信息执行任务，那么该信息是有效的。这对应于以下信息质量目标：适量、相关性、可理解性、解释性、客观性
效率	虽然有效性把信息视为一种产品，效率更多地与获取和使用信息有关，所以它与“信息作为一种服务”的观点相一致。如果满足信息消费的需求的信息可以用一种简单的方法获得和使用，那么信息的使用是高效的。这对应于以下信息质量目标：可信度、可访问性、易于操作、信用度
完整性	如果信息具有完整性，那么它是没有错误的、完整的

企业需要如何做，它是一个控制架构而非具体如何操作的过程架构。ITIL 基于企业的最佳实践，OGC 收集和分析各种组织解决服务管理问题方面的信息，找出那些对本部门和对英国政府其他部门有益的作法，最后形成了 ITIL。它列出了各个服务管理流程“最佳”的目标、活动、输入和输出以及各个流程之间的关系，但没定义范围广泛的控制架构。它关注方法和实施过程。尽管两个标准有着许多的不同之处，但在 COBIT 和 ITIL 背后却有着非常一致的指导原则。信息系统审计师通常综合使用 COBIT 和 ITIL 的自评估方法，评估企业 IT 服务管理环境。COBIT 为每一个过程提供了关键目标指标（KGIs）、关键绩效指标（KPIs）、关键成功要素（CSFs），这些指标与 ITIL 过程相结合，可以建立 ITIL 过程管理的基准。在实际应用中，某些企业综合两个标准提出了更易理解的、适用于本企业环境的 IT 治理和运行架构。

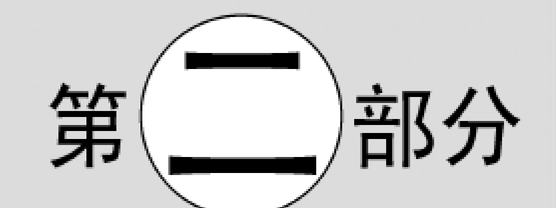
与 ISO 27001 不同，COBIT 完全基于信息技术，其 IT 准则反映了企业的战略目标，IT 资源包括人、系统、数据等相关资源，IT 管理则是在 IT 准则指导下对 IT 资源进行规划处理。

PRINCE2 为包括 IT 项目在内的项目管理提供了通用的管理方法，内置了在项目管理实践中已证明成功的最佳实践，通过为所有参与者提供的通用语言，便于被广泛理解和接受。COBIT 从战略、战术、技术等层面给出了如何有效管理 IT 项目。除给出项目管理的具体控制目标外，COBIT 还给出了与项目管理相关的关键成功要素，其定义了最重要的面向项目管理的实施指南，以达到对 IT 项目过程内外部的控制；关键目标指标定义了一些尺度，便于在项目关键点，告诉管理者某个 IT 项目管理过程是否实现了其业务需求；关键绩效指标定义的是 IT 项目管理过程在促使项目目标达成时履行得有多好的尺度。从两者的比较可以看出，COBIT 重点在于对控制目标的管理上，PRINCE2 典型的在于对流程的管理上。虽然二者从不同的角度出发认识 IT 项目管理，但二者有许多共同之处。COBIT 的项目中主要计划，系统质量保证计划，保证方法计划，测试计划，培训计划，实施后的评审计划等控制目标映射到 PRINCE2 的计划流程；项目管理架构等映射到 PRINCE2 的指导项目流程；PRINCE2 的开始项目和启动项目流程对应着 COBIT 的用户方参与项目启动，项目团队身份及其职责，项目定义；项目批准，项目阶段批准，正式的项目风险管理则较好地被其他几个 PRINCE2 流程所包含。PRINCE2 从流程的角度对项目管理中各个活动进行管理，比较便于项目管理的具体实施，而 COBIT 从控制目标的角度阐述项目管理“应该怎样，应该达到什么目标”，这样便于企业控制和评审项目管理整体过程的执行情况。

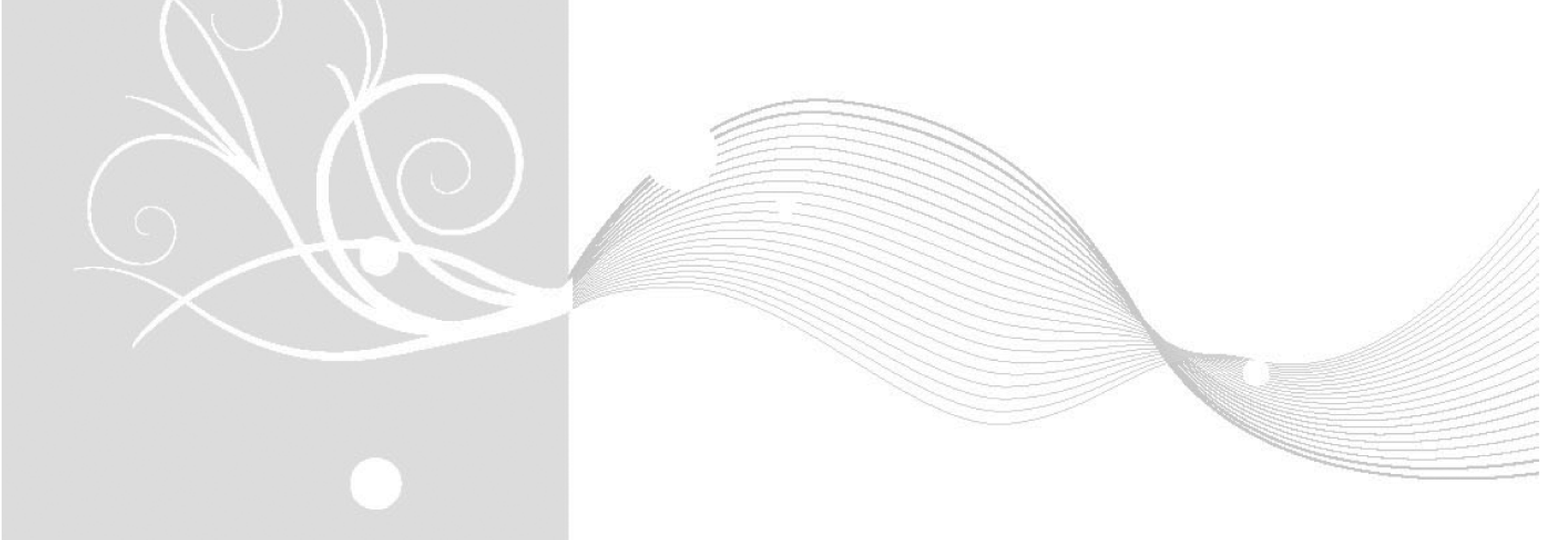
COBIT、ITIL、ISO/IEC 27001 和 PRINCE2 在管理 IT 上各有优势，如 COBIT 重点在于 IT 控制和 IT 度量评价；ITIL 重点在于 IT 过程管理，强调 IT 支持和 IT 交付；ISO/IEC 27001 重点在于 IT 安全控制；PRINCE2 重点在于项目管理，强调项目的可控性，明确项目管理中人员角色的具体职责，同时实现项目管理质量的不断改进。

思考题

1. 简单叙述 IT 治理的基本概念。
2. 简单叙述你对 IT 治理与 IT 管理的理解。
3. 查阅资料，归纳 IT 治理支持手段。
4. 什么是 ITIL？其包括哪些管理流程？
5. 简单叙述 COBIT 5.0 的 5 个原则和 7 个驱动因素。



信息安全风险评估



第5章 信息安全风险评估实施流程

5.1 风险评估准备

风险评估的准备是整个风险评估过程有效性的保证。组织实施风险评估是一种战略性的考虑,其结果将受到组织的业务战略、业务流程、安全需求、系统规模和结构等方面的影响。因此,在风险评估实施前,组织应当做到以下几点:

1. 确定风险评估的目标

根据满足组织业务持续发展在信息安全方面的需要、法律法规的规定等内容,识别现有信息系统及其管理上的不足,以及可能造成的风险大小。

2. 确定风险评估的范围

风险评估范围可能是组织全部的信息及与信息处理相关的各类资产、管理机构,也可能是某个独立的信息系统、关键业务流程、与客户知识产权相关的系统或部门等。

3. 组建评估团队

风险评估实施团队是由管理层、相关业务骨干、IT技术等人员组成的风险评估小组。必要时,可组建由评估方、被评估方领导和相关部门负责人参加的风险评估领导小组,聘请相关专业的技术专家和技术骨干组成专家小组。

评估实施团队应做好评估前的表格、文档、检测工具等各项准备工作,进行风险评估技术培训和保密教育,制定风险评估过程管理相关规定。可根据被评估方要求,双方签署保密合同,适情签署个人保密协议。

4. 进行系统调研

系统调研是确定被评估对象的过程,风险评估小组应进行充分的系统调研,为风险评估依据和方法的选择、评估内容的实施奠定基础。调研内容至少应包括:

(1) 业务战略及管理制度。

(2) 主要的业务功能和要求。

(3) 网络结构与网络环境,包括内部连接和外部连接。

(4) 系统边界。

(5) 主要的硬件、软件。

(6) 数据和信息。

(7) 系统和数据的敏感性。

(8) 支持和使用系统的人员。

(9) 其他。

系统调研可以采取问卷调查、现场面谈相结合的方式进行。调查问卷是提供一套关于管理或操作控制的问题表格，供系统技术或管理人员填写；现场面谈则是由评估人员到现场观察并收集系统在物理、环境和操作方面的信息。

5. 确定评估依据和方法

根据系统调研结果，确定评估依据和评估方法。评估依据主要包括：

(1) 现有国际标准、国家标准、行业标准。

(2) 行业主管机关的业务系统的要求和制度。

(3) 系统安全保护等级要求。

(4) 系统互联单位的安全要求。

(5) 系统本身的实时性或性能要求等。

根据评估依据，应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险计算方法，并依据业务实施对系统安全运行的需求，确定相关的判断依据，使之能够与组织环境和安全要求相适应。

6. 制定评估方案

风险评估方案的目的是为后面的风险评估实施活动提供一个总体计划，用于指导实施方开展后续工作。风险评估方案的内容一般包括以下几方面。

(1) 团队组织：包括评估团队成员、组织结构、角色、责任等内容。

(2) 工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容。

(3) 时间进度安排：项目实施的时间进度安排。

7. 获得最高管理者支持

上述所有内容确定后，应形成较为完整的风险评估实施方案，得到组织最高管理者的支持、批准；对管理层和技术人员进行传达，在组织范围内就风险评估相关内容进行培训，以明确有关人员在风险评估中的任务。

5.2 资产识别

识别阶段的主要工作是：识别信息安全风险的主要构成要素——资产、威胁、脆弱性，以及分析和确定已有安全控制措施的有效性。经过识别阶段采集到的上述信息，在分析阶段将被用于风险分析的输入数据。识别阶段获得的原始信息越翔实，就越能保证风险分析结果的客观性和相应建议的针对性，被评估组织就能从评估活动中获得更大的安全收益。

信息资产是具有价值的信息或资源，它能够以多种形式存在，有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等。保密性、完整性和可用性是评价信息资产的三个安全属性。风险评估中资产的价值不仅以资产的经济价值来衡量，而且由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定。

但在实际客户环境中，信息系统可能会非常复杂，划分了大量的子系统、应用以及模块，并包括各种元素。若对资产仅进行笼统的划分，对于真正的评估没有任何意义，而进行笼统划分得到的最终评估结果往往只是对单台设备的漏洞检查和分析，或是单条制度的修改，无法从整体意义或是不同客户群体关心的问题出发，得到相应的安全等级划分，以及进一步的安全建议或技术方案。因此，在资产识别过程中，除了要对资产进行合理分类之外，还应体现出资产之间的关联和层次。

5.2.1　工作内容

信息资产作为信息系统的构成元素，分布十分广泛，不同信息资产的功能、重要程度也互不相同。因此，需要对信息资产进行合理分类，分析安全需求，确定资产的重要程度。本部分的主要工作是在评估实施方案确定的范围之内，按照评估方案约定的方式，进行如下4项工作。

1. 回顾评估范围内的业务

回顾这些信息的主要目的是：帮助资产识别小组对其所评估的业务和应用系统有一个大致了解，为后续的资产识别活动做准备。如果在准备阶段已就这部分信息进行过交流并生成了相应的描述性的文档，这部分工作不必重复进行，直接阅读该描述性文档即可。

2. 识别信息资产，进行合理分类

针对前一个活动中识别出来的每个主要业务或系统，识别完成业务或保证系统正常运转所必需的资产，并注明资产的类别。资产分类的目的是为后续工作做准备、降低后续分析和赋值活动的工作量。

3. 确定每类信息资产的安全需求

在对资产进行合理分类之后，便可从保密性、完整性和可用性三个方面对每种资产类别进行安全需求分析，而不是对每个资产进行安全需求分析。

4. 为每类信息资产的重要性赋值

在上述安全需求分析的基础上，按照一定方法，确定资产的价值或重要程度等级。

5.2.2　参与人员

资产识别阶段主要参与人员包括：来自评估单位的项目负责人和资产识别小组，以及各活动中来自被评估组织的被访谈人员。被访谈人员与本阶段各活动的对应关系如下所述。

(1) 回顾评估范围之内的业务和系统。参与此活动的被访谈人员,应了解被评估组织的业务特点以及支撑业务运转的信息系统的架构。

(2) 识别信息资产进行合理分类。此项活动主要由评估单位来完成,但也可以考虑邀请被评估组织的项目负责人加入此项活动。

(3) 确定每类信息资产的安全需求。此项活动应邀请资产所有者或负责人加入。

(4) 为每类信息资产的重要性赋值。此项活动由资产识别小组负责,需要被评估组织的人员参与。

被评估组织的项目负责人负责上述工作的协调。

5.2.3 工作方式

1. 评估范围之内的业务识别

同一个组织有多种不同的业务,不同的业务部门分别进行不同的活动来共同实现组织的经营目标。然而组织的各种业务在组织整体经营活动中的重要程度不同,因此,为便于评估报告的分析和对比,要将组织各项业务按其重要性级别赋值。表 5-1 为一个简单示例,其中,5 为重要性最高、1 为最低。用户可根据自己的实际情况和需要来具体赋值。

表 5-1 业务重要性级别调查表

业务名称	业务描述	重要性级别
仓储	产品库存和资产保管	4
生产	产品制造和生产	5
研发	新产品和技术的研究与开发	4
财务	企业财务管理	3
销售	产品和服务销售	4
人事	人员招聘和工资管理等	3
行政	后勤等服务管理	1
宣传	企业对外宣传等	2

2. 资产的识别与分类

每个类别的资产都具有一定的安全属性;同一资产类别中的不同资产之间安全属性的差别是将每个资产类别进一步划分为多个信息资产子类的依据。《信息安全风险评估规范》中给出了基于表现形式的资产分类方式,见表 5-2。

在对资产进行分类时,应遵循以下原则:分类方法简单、直观,全面覆盖、避免重叠。业务和资产的识别工作通常经由业务部门实现,支持业务应用的关键资产要通过对文档的审核以及跟业务部门的管理者和相关业务、技术人员的面谈来进行。工作流程要确保资产识别过程的一致性,识别内容包括物理资产和地点、网络和逻辑连接、软件(操作系统和应用软件等)、通过网络传送的数据流等。访谈的重点应集中于信息资产如何被各种类型的用户(如系统管理员、客户和雇员等)所使用。表 5-3 给出了一个业务单元信息资产调查表的例子。

表 5-2　《信息安全风险评估规范》中基于表现形式的资产分类方式

分类	示　　例
数据	保存在信息媒介上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等
软件	系统软件：操作系统、语言包、工具软件、各种库等。 应用软件：外部购买的应用软件、外包开发的应用软件等。 源程序：各种共享源代码、自行或合作开发的各种代码等
硬件	网络设备：路由器、网关、交换机等。 计算机设备：大型计算机、小型计算机、服务器、工作站、台式计算机、移动计算机等。 存储设备：磁带机、磁盘阵列、磁带、光盘、移动硬盘等。 传输线路：光纤、双绞线等。 保障设备：动力保障设备(UPS、变电设备等)、空调、保险柜、文件柜、门禁、消防设施等。 安全保障设备：防火墙、入侵检测系统、身份验证等。 其他：打印机、复印机、扫描仪、传真机等
服务	办公服务：为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等服务。 网络服务：各种网络设备、设施提供的网络连接服务。 信息服务：对外依赖该系统开展的各类服务
文档	纸质的各种文件，如传真、电报、财务报告、发展计划等
人员	掌握重要信息和核心业务的人员，如主机维护主管、网络维护主管及应用项目负责人等
其他	企业形象、客户关系等

表 5-3　信息资产调查表举例

财务部门信息资产调查表	
1. 系统和应用软件	
应用系统	现金管理系统、账务管理系统
操作系统	Windows XP、Windows 2003 Server
其他	
2. 硬件	
服务器	HP
网络和通信设备	Cisco2600 路由器、Cisco3550 交换机、调制解调器
个人计算机	联想、DELL
其他设备	HP 打印机
3. 其他信息资产	
备份数据	磁带
纸质文档和文件	
其他移动数据存储	
备注	PDA、U 盘、笔记本

至于各个具体的信息资产，如操作系统、服务器硬件等，还需要进一步对其进行设备厂家、型号、CPU、内存、操作系统类型、版本号、当前已安装补丁版本号等进行详细调查

统计。

3. 安全需求分析

根据被分析的资产类别在其业务或应用系统中的位置以及所发挥的作用，分析每个资产类别在保密性(C)、完整性(I)和可用性(A)三个方面的要求。

此项活动中，来自资产识别小组成员和被评估组织的参与人员的意见都应予以考虑。当双方面人员发生意见分歧时，双方项目负责人应促使双方达成共识。

4. 资产赋值

为了后续风险计算过程的需要，必须对资产进行赋值。对资产进行赋值不仅需要考虑它本身的财务价值，还要考虑它的损失可能会对业务造成的影响，如导致营业收入的减少或竞争对手得益等。甚至有时相对于对组织业务的影响造成的损失而言，损失资产本身的物理价值可以忽略不计。举个例子来说：美国微软公司若丢失了一台存有最新 Windows 服务器版的操作系统源代码的笔记本，这个丢失事件的发生对微软公司业务造成的损失要比资产本身(笔记本)的价值要大得多。

风险评估方法一般包括定量评估和定性评估两种方法。定量评估中对资产本身的财务价值和其本身会对业务造成的影响损失来综合赋值，而在许多情况下，资产本身的财务价值相对于企业业务损失影响所占比例非常小。为了分析的简化和方便，许多企业在风险评估时干脆就不考虑资产本身的财务价值了。但是对一些中小企业而言，资产本身的财务价值就不能不加以考虑，这时就需要结合起来进行综合赋值。这两种方式用户可以根据需要，自由考虑选用。

国外流行的一些定量风险评估方法通常将资产按其经综合考虑后的财务价值来这样赋值，如：

1 表示 1～100 元；

2 表示 101～1000 元；

3 表示 1001～10 000 元；

……

而定性风险评估一般将资产按其对于业务的重要性来这样赋值：

1 表示极低；

2 表示低；

3 表示中；

4 表示高；

5 表示极高。

参考以上两种方法的优点，可采用如表 5-4 所示的方法对信息资产赋值。(注：重要性级别 10 为最高、1 为最低。)

这样，无论用户根据需要采用定量评估还是定性评估，这个信息资产赋值方法不需修改就都能适用，大大增加了它的适用性和统一性。

表 5-4　信息资产赋值表

资产赋值	经综合考虑后的财务价值	对于业务的重要性级别
1	1～100 元	1
2	101～1000 元	2
3	1001～10 000 元	3
4	10 001～100 000 元	4
5	100 001～1 000 000 元	5
6	1 000 001～10 000 000 元	6
7	10 000 001～100 000 000 元	7
8	100 000 001～1 000 000 000 元	8
9	1 000 000 001～10 000 000 000 元	9
10	10 000 000 001～100 000 000 000 元	10

5.2.4　工具及资料

资产识别活动中，可能会使用到下述工具或资料。

1. 自动化工具

尽管目前尚不存在可以完成资产识别活动的自动化工具，但可以借助一些资产管理工具或带有资产识别和管理功能的其他安全产品，如扫描工具、SOC 或专门为评估订制的工具等，快速完成资产识别活动，缩短本活动所占用的时间。

1）资产管理工具

尽管不太常见，但市场上确实存在专门的资产管理产品或解决方案。这类产品专门为企业用户设计，便于管理员管理企业的 IT 资产，被管理的对象主要是主机（包括其中的操作系统和应用程序）和网络设备，这些被管理对象一般都具有 IP 地址。某些较为高级的产品具有拓扑结构发现功能。

为了实现更多的管理功能，需要在被管理的服务器或客户端上安装相应的代理程序。征得被评估单位的同意后，才可以使用资产管理工具来完成资产识别工作。

另外，更加复杂的安全解决产品或方案，可能具有用于资产管理的功能模块，例如 SOC。

2）主动探测工具

对于评估单位来说，更倾向于使用一些可以针对 IT 资产进行主动探测的工具。因为使用这类产品无须在被评估组织的实际业务系统中大规模部署。

目前一些较为先进的漏洞扫描工具，在专门的扫描策略下，可以完成对绝大部分 IT 资产的精确辨别（被辨别或被识别的对象应该具有各自的 IP 地址），这样就可以省去资产识别人员大量的现场调查和访谈工作，大大节约资产识别活动花费的时间。

根据相关标准对信息资产的定义，信息资产并非仅限于带有 IP 地址的信息系统组件，通常还会包括人员、数据存储介质、文档、线路、非 IT 辅助设备等。而这些对象都无法被前面提到的两类工具自动发现。因此，实际评估项目中，还需要人工完成上述资产的识别活动。

2. 手工记录表格

在资产识别活动中，评估单位需要提供用于资产识别活动的记录表格(示例见表 5-5)。以下人工资产识别活动的记录表格仅供参考，可根据评估活动的实际情况或用户要求，对表格中的记录项进行增加或删除。

表 5-5　资产识别记录表格示例

资产识别记录表			
项目名称或编号		表格编号	
资产识别活动信息			
日期		起止时间	
访谈者		访谈对象及说明	
地点说明			
记录信息			
所属业务		业务编号	
所属类别		类别编号	
资产名称		资产编号	
IP 地址		物理位置	
功能描述			
保密性要求			
完整性要求			
可用性要求			
重要程度			
安全控制措施			
负责人			
备注			

3. 辅助材料

被评估组织应提供最新的、详细的网络拓扑图，以及行业运行流程图，这有助于资产识别活动的开展，还可以避免在资产识别过程中发生遗漏。

如果被评估组织以前曾经进行过风险评估，可以在上个评估活动生成的资产识别列表的基础上，仅对变更的资产进行识别，也可大大节约本阶段所需要的时间，提高工作效率。

5.2.5　输出结果

在资产划分的基础上，再进行资产的统计、汇总，形成完备的《资产及评价报告》。此报告属于评估活动的中间结果，将被视为分析阶段的输入文档之一。在评估方案中，如果未明确指明此报告需要作为中间结果提交给被评估方，那么此报告可以不必提交给被

评估组织。

5.3　威胁识别

根据《信息安全风险评估规范》对应部分的阐述："威胁是一种对组织及其资产构成潜在破坏的可能性因素，是客观存在的。"

威胁是构成信息安全风险不可缺少的要素之一：在信息资产及其相关资产存在脆弱性和相应的安全控制措施缺失或薄弱的条件下，威胁总是通过某种具体的途径或方式，作用到特定的信息资产之上，并破坏该资产一个或多个安全属性，从而产生信息安全风险。

威胁识别主要是识别被评估组织或资产直接或间接面临的威胁，以及相应的分类和赋值等活动。威胁识别活动的主要目的是建立风险分析所需要的威胁场景。

5.3.1　工作内容

1. 威胁识别

(1) 实际威胁识别：通过访谈和检测工具识别并记录被评估组织近期曾经实际出现过的威胁。

(2) 潜在威胁识别：根据被评估组织的特点，结合当前信息安全总体的威胁统计和趋势，分析被评估组织面临的潜在威胁。

2. 威胁分类

对上述实际发生过的和潜在的威胁进行分类。与资产分类的目的类似，对威胁进行分类可以简化后续分析、赋值和计算等活动的工作量。

3. 威胁赋值

某些具体的风险计算方法，需要在这个阶段中对威胁进行赋值。因此，需要对具体威胁或威胁类别进行赋值，作为后续计算的输入。

4. 构建威胁场景

在前面威胁识别和威胁分类的基础上，为每个或每类关键资产构建威胁场景图。

5.3.2　参与人员

威胁识别活动的主体是评估团队中的威胁识别小组。另外，在实际威胁调查的活动中(如访谈和工具检测)，还需要来自于被评估组织的人员参与。

(1) 访谈：关键资产的所有者或负责人作为访谈对象。

(2) 工具检测：被检测网络的管理员、被检测系统的管理员。

被评估组织的项目负责人负责上述本方人员的落实。

5.3.3 工作方式

1. 威胁识别

1）针对实际威胁的识别活动

本活动的目的是：识别并记录被评估组织实际发生过的威胁。完成此活动可以通过人员访谈和工具检测两种方式。

人员访谈方式可以使威胁识别小组快速地了解被评估组织近期发生过何种威胁。被访谈的对象应是关键资产的所有者或负责人。通过面对面交流，围绕特定的关键资产或资产类别，威胁识别小组成员可以从被访谈对象口中，直接获得关键资产曾经遭受过哪些具体威胁的破坏，或对一些安全事件表面现象进行分析后，间接获得安全事件背后的威胁源头。在进行人员访谈时，应指定威胁小组中的一位成员负责访谈过程中的记录工作。

由于能力或手段上的局限，被评估组织人员无法察觉所有实际发生过的威胁。这就需要依靠威胁识别小组成员的专业技能或使用专业的工具来检测这些不易察觉的威胁。工具检测活动主要从网络流量和日志两个方面入手。

从网络流量入手是通过对网络流量进行不间断地分析，从中发现攻击、入侵或非法访问等行为。一般使用 IDS（设备或软件形式均可）来完成这项工作的；条件允许时，还可以考虑使用协议分析工具，来检测网络中的异常活动。如果被评估组织已经部署了上述工具，威胁小组可以直接获取检测结果。而从日志记录入手的原理在于，信息系统各组件一般都具有丰富的审计能力并生成日志记录，威胁识别小组可以利用日志分析工具，从这些日志记录中，快速地获取威胁信息。

上面两种威胁识别活动，应采取统一的格式记录被识别的威胁。记录中应包含以下信息：

（1）关键资产名称或类别名称。

（2）工具检测活动的说明信息：时间、地点和检测方式。

（3）威胁主体。

（4）威胁来源或方位。

（5）途径和方式说明。

（6）现象（如次数、周期等）。

（7）结果和影响。

（8）后续补救措施。

需要注意的是，应将工具检测过程中的原始数据全部保留下来，便于被评估组织日后的核查和加固工作。针对那些对安全性和实时性要求非常苛刻的系统进行威胁识别时，使用工具检测需要谨慎。另外，工具检测内容毕竟有限，所以可能需要威胁识别小组成员对被评估的系统或设备进行更深入的人工检查。

2）针对潜在威胁的识别活动

上述针对实际威胁的识别活动，只能发现那些曾经发生过的威胁。某些威胁从未发生过，并不意味着这些威胁永远不会出现。而且，随着技术的发展，总会有新的威胁出现；组织业务和信息系统的调整，也可能会引入新的威胁。所以，除了识别实际威胁外，还应根据

当前总体的威胁态势，识别被评估组织面临的一些潜在威胁。

经过准备阶段中“前期系统调研”活动，评估团队主要成员已经对被评估组织的业务、信息系统(包括主要的安全技术控制措施)、组织和人员等方面有了基本了解。在此基础上，威胁识别小组成员通过对整体威胁态势的掌握和依靠外部威胁的统计报告，结合被评估组织的实际情况，便可大致确定被评估组织面临的潜在威胁。

既然此项活动识别的是潜在威胁，这就意味着这种威胁可能发生，也可能不发生。被评估单位的人员就会对此项活动的识别结果产生不同程度的怀疑。那么，对于每个被识别出来的潜在威胁，评估人员应提供详细的描述和实例，以说明潜在威胁分析、识别的结论。通常可以从以下几个方面说明理由。

威胁途径：根据被评估组织的实际情况，描述出某种威胁具备发生或传播的途径。

防护措施：安全防护或检测措施的缺失或薄弱，使得某种威胁有可乘之机。

威胁动机：组织通常将绝大部分的安全投资用于抵御外部威胁，而对于其内部人员控制措施较薄弱，同时无法排除内部人员具有不良动机。

外部统计数据：国际和国内的一些机构，如国家计算机网络应急技术处理协调中心，会在 http://www.cert.org.cn 网站上定期发布安全公告和阶段性安全事件的统计数据。这些数据对被评估单位进行威胁分析很有帮助。

潜在威胁识别记录内容应包括：

(1) 威胁主体和动机。

(2) 威胁来源或方位。

(3) 途径和方式说明。

(4) 缺失或薄弱的安全控制措施。

(5) 威胁的客体。

(6) 可能的结果。

(7) 后续补救措施。

2. 威胁分类

对已经发生过的和潜在的威胁进行分类。与资产分类的目的类似，对威胁进行分类可以简化后续分析、赋值和计算等活动的工作量。

《信息安全风险评估规范》给出了两种威胁分类的方式：一种是基于来源对威胁进行分类，见表 5-6；一种是基于表现形式对威胁进行分类，见表 5-7。

3. 构建威胁场景

在前面威胁识别和威胁分类的基础上，接下来需要为每个关键资产或关键资产类别构建威胁场景图，为后续的风险分析/计算活动进一步缩小范围。

威胁场景实质上是：为每个关键资产或关键资产类别与其所面临的实际和潜在威胁建立对应关系。这样做可以获得以下两个方面的益处：首先，排除掉那些不可能存在的“关键资产-威胁”对，避免在后续的风险分析/计算活动中，浪费时间和人力；其次，威胁场景除了建立起关键资产与其面临威胁之间的对应关系外，还明确了威胁的来源、途径和结果，有助于后续风险分析阶段结合脆弱性和已有的安全控制措施进行影响和可能性分析。

表 5-6 《信息安全风险评估规范》中基于来源的威胁分类表

来　　源		描　　述
环境因素		由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件或自然灾害，意外事故或软件、硬件、数据、通信线路方面的故障
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏； 采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益； 外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进行破坏，以获取利益或炫耀能力
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏； 内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击

表 5-7 《信息安全风险评估规范》中基于表现形式的威胁分类表

种　　类	描　　述	威 胁 子 类
软硬件故障	由于设备硬件故障、通信链路中断、系统本身或软件缺陷造成对业务实施、系统稳定运行的影响	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障
物理环境影响	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题或自然灾害	
无作为或操作失误	由于应该执行而没有执行相应的操作或无意地执行了错误的操作，对系统造成的影响	维护错误、操作失误
管理不到位	安全管理无法落实、不到位，造成安全管理不规范或者管理混乱，从而破坏信息系统正常有序运行	
恶意代码和病毒	具有自我复制、自我传播能力，对信息系统构成破坏的程序代码	恶意代码、木马后门、网络病毒、间谍软件、窃听软件
越权或滥用	通过采用一些措施，超越自己的权限，访问了本来无权访问的资源，或者滥用自己的职权，做出破坏信息系统的行为	未授权访问网络资源、未授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄漏秘密信息
网络攻击	利用工具和技术，如侦察、密码破译、安装后门、嗅探、伪造和欺骗、拒绝服务等手段，对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探(账户、口令、权限等)、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃
泄密	信息泄漏给不应了解的他人	内部信息泄漏、外部信息泄漏
篡改	非法修改信息、破坏信息的完整性，使系统的安全性降低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息
抵赖	不承认收到的信息和所作的操作和交易	原发抵赖、接收抵赖、第三方抵赖

一旦威胁突破了已有的安全控制措施，利用了资产（或其相关资产）的脆弱性，就会对该资产的某个或某些安全属性造成破坏，从而导致以下不期望的结果发生：

（1）泄漏——保密性（C）遭破坏，主要针对数据类的资产。

（2）篡改——完整性（I）遭破坏，主要针对数据类或软件类的资产。

（3）中断——可用性遭破坏（A），主要指网络通信和服务。

（4）损失或破坏——可用性遭破坏（A），主要指数据、软件和物理形式的资产。

4．威胁赋值

对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。如果不考虑其他因素（例如，资产、脆弱性和已有的安全措施以及被评估组织其他实际情况）而单纯地对威胁进行评价或赋值，就势必会割裂风险构成要素之间的内在联系，使得后面的风险计算结果的可信程度受到置疑。所以威胁识别要与资产识别相联系。

威胁识别要从威胁源、事件发生后对信息资产的影响程度（或造成的损失）和事件发生的可能性等多方面来考虑。某个信息资产面临的单个威胁综合值计算公式为：

$$t = T_s + T_i$$

其中，t 为单个威胁综合值，T_s 为威胁来源值，被定义为一个 1～5 之间的数值，T_i 为影响程度值，也被定义为一个 1～5 之间的数值，因此可以计算出某个信息资产面临的单个威胁综合值。

威胁来源值 T_s：按照威胁性级别的不同可定义为 1～5 的数值。暂时定为将每一个威胁都为它分配一个威胁来源值，这样在以后的计算中，就可以根据用户对威胁的选择来自动计算威胁综合值了。威胁源示例必须补充，分配给每一个威胁源。

影响程度值 T_i：按照安全事件发生后会对业务产生的影响，暂时定为让用户来选择，让用户看到定义，根据实际情况来选择影响程度值。

综上所述，一个信息资产面临的所有威胁综合值，等于所有单个威胁综合值相加后除以威胁个数的 2 倍，再将此计算结果四舍五入，最后的结果是一个 1～5 之间的整数。计算公式如下：

$$T = \mathrm{INT}\left\{\sum_{i=1}^{N}(t_i)\right\}/2N + 0.5$$

例如，某一信息资产共有 5 个威胁源，它们各自的威胁来源值和影响程度值见表 5-8。

表 5-8 某一信息资产各威胁源的威胁来源值和影响程度值

威胁源	威胁来源值 T_s	影响程度值 T_i	单个威胁综合值 t
威胁 T_1	1.5	3.5	5.0
威胁 T_2	3.7	4.0	7.7
威胁 T_3	2.3	0.5	2.8
威胁 T_4	2.2	3.0	5.2
威胁 T_5	1.9	1.5	3.4

由表中已知数据可得 5 个威胁源的单个威胁综合值相加后的和为 $\sum_{i=1}^{5}(t_i)=24.1$，从而该信息资产面临的所有威胁综合值为 $T=3$。

5.3.4 工具及资料

在针对实际威胁识别活动中，可能会使用 IDS、安全审计等工具，以及人员访谈所需的记录表格。

5.3.5 输出结果

（1）威胁列表。
（2）关键资产的威胁场景。

5.4 脆弱性识别

脆弱性是指资产中可能被威胁所利用的弱点，包括技术脆弱性和管理脆弱性两种。

5.4.1 工作内容

各类技术脆弱性的存在，势必会大大增加安全事件发生的可能性，从而加大信息系统整体的安全风险。因此，需要对信息系统中当前的脆弱性进行识别，脆弱性识别应包括以下活动。

脆弱性识别：通过扫描工具或手工等不同方式，识别当前系统中存在的脆弱性。

识别结果整理与展示：在实际评估项目中，被评估组织往往会要求评估单位提交脆弱性识别活动的阶段成果，所以在脆弱性识别阶段，还应将脆弱性识别结果以合理的方式展现给被评估组织。

脆弱性赋值：某些具体的风险分析、计算方法，需要对脆弱性赋值后方能完成后续的风险计算活动。如果评估活动选用了上述类型的风险分析、计算方法，应根据一定的赋值准则，对被识别的脆弱性进行赋值。

5.4.2 参与人员

本部分具体活动与参与人员的对应关系见表 5-9。

表 5-9 脆弱性识别工作的参与人员

序号	活动名称	参与人员	
		来自于评估单位	来自于被评估单位
1	脆弱性识别	项目负责人 脆弱性识别小组	项目负责人 识别活动中配合人员或访谈对象
2	脆弱性识别结果整理与展现	脆弱性识别小组	
3	脆弱性赋值	脆弱性识别小组	

5.4.3　工作方式

1. 脆弱性识别方法

依据《信息安全风险评估规范》相关内容的阐述，脆弱性识别所采用的方法主要有：

(1) 问卷调查。

(2) 工具检测。

(3) 人工检查。

(4) 文档查阅。

(5) 渗透性测试，等。

其中，工具检测具有非常高的效率，因而是在实际评估项目中评估单位大都会选用的一种方式。但考虑到工具扫描具有一定风险，在对那些对可用性要求较高的重要系统进行脆弱性识别时，经常会使用人工检查的方式。

2. 脆弱性识别原则

在识别信息系统的脆弱性时，需要坚持以下原则：

1) 全面考虑和突出重点相结合的原则

由于脆弱性可能存在于系统的任何环节、任何部位，所以识别时要进行全面的考虑，仔细考察每一个因素。可以从信息系统的共性总结出共通的脆弱性。但是，每个信息系统都有其独有的特点，其所处环境、服务对象和目的、系统结构、提供服务和操作人员各不相同，所具有的脆弱性也各有侧重，需要针对具体系统做具体分析，从组织的实际需求出发，从业务角度进行识别，兼顾安全管理和业务运营。

2) 局部与整体相结合的原则

信息系统是由硬件设备及其软件、应用服务、文档等对象组成的一个整体，系统中任何元素的脆弱性都会造成整个系统的脆弱性。因此，确定信息系统的脆弱性时，必须考虑每个主机和设备甚至其单个组件的脆弱性。但这并不够，因为复杂的信息系统是组成它的各个元素相互作用的结果，所有元素本身不存在脆弱性并不能保证它们交互的结果——整个系统不会产生新的脆弱性。所以，从微观的角度考察各个组成元素的同时，更需要从整体上、从系统的层面来辨识脆弱性。

3) 层次化原则

国际标准化组织在开放系统互连标准中定义了包含 7 层的网络互连参考模型，不同的层次完成不同的功能。现有网络信息系统架构基本上遵循这一标准，因此，为了保障系统的安全性，需要在各层分别提供不同的安全机制和安全服务。相应地，系统在各个层次上都可能存在脆弱性，而且脆弱性也具有层次性，评估时必须考虑层次化特点。

4) 手工与自动化工具相结合的原则

当前已经出现许多脆弱性自动扫描工具，工具的使用可大大减轻手工劳动的强度，加快进度，但在涉及管理方面的问题时，工具往往无能为力。例如，人员管理、制度等方面的脆弱性往往难以通过工具识别。而且目前的识别工具大多只是进行局部识别，最多也只是能够对单一主机的多种组件进行简单的相关检查，对多台主机构成的网络信息、系统进行有效的

脆弱性识别目前还无能为力,只能依靠人力完成。通过问卷调查、会议、访谈、专家检查、网上脆弱性信息、渗透测试、入侵检测、审计和自评估等方法识别出系统的脆弱性后,还需要对这些脆弱性进行等级赋值,由被威胁利用的可能性和可能造成资产损失的严重性确定,脆弱性被利用和造成损失程度越高,所应赋的等级也越高,通过对照标准表可以确定所有脆弱性的等级。

3. 脆弱性识别内容

脆弱性是资产本身存在的,如果没有被相应的威胁利用,单纯的脆弱性本身不会对资产造成损害。而且如果系统足够强健,严重的威胁也不会导致安全事件发生,并造成损失。即,威胁总是要利用资产的脆弱性才可能造成危害。资产的脆弱性具有隐蔽性,有些脆弱性只有在一定条件和环境下才能显现,这是脆弱性识别中最为困难的部分。不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个脆弱性。

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心,针对每一项需要保护的资产,识别可能被威胁利用的弱点,并对脆弱性的严重程度进行评估;也可以从物理、网络、系统、应用等层次进行识别,然后与资产、威胁对应起来。脆弱性识别的依据可以是国际或国家安全标准,也可以是行业规范、应用流程的安全要求。对应用在不同环境中的相同的弱点,其脆弱性严重程度是不同的,评估者应从组织安全策略的角度考虑、判断资产的脆弱性及其严重程度。信息系统所采用的协议、应用流程的完备与否、与其他网络的互联等也应考虑在内。

脆弱性识别时的数据应来自于资产的所有者、使用者,以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有:问卷调查、工具检测、人工核查、文档查阅、渗透测试等。脆弱性识别主要从技术和管理两方面进行,技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面,前者与具体技术活动相关,后者与管理环境相关。对不同的识别对象,其脆弱性识别的具体要求应参照相应的技术或管理标准实施。例如,对物理环境的脆弱性识别应按 GB/T 9361 中的技术指标实施;对操作系统、数据库应按 GB 17859—1999 中的技术指标实施。对管理脆弱性识别方面应按 GB/T 19716—2005 的要求对安全管理制度及其执行情况进行检查,发现管理漏洞和不足。

4. 脆弱性赋值

可以根据对资产的损害程度、技术实现的难易程度、弱点的流行程度,采用等级方式对已识别的脆弱性的严重程度进行赋值。由于很多弱点反映的是同一方面的问题,或可能造成相似的后果,赋值时应综合考虑这些弱点,以确定这一方面脆弱性的严重程度。

对某个资产,其技术脆弱性的严重程度还受到组织管理脆弱性的影响。因此,资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。脆弱性严重程度可以进行等级化处理,不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大,脆弱性严重程度越高。将脆弱性基于严重性分级,对计算出的结果可以按表 5-10 进行定义。

表 5-10　脆弱性等级表

等　级	表　示	定　义
3	高	如果被威胁利用,将对资产造成完全破坏的结果
2	中	如果被威胁利用,将对资产造成一般损害的结果
1	低	如果被威胁利用,将对资产造成的损害可以忽略

与威胁识别相同,脆弱性的识别也要针对资产,并且还要求资产必须已存在威胁,这样才能正确地完成风险评估的任务,同时也可以让使用该系统的用户了解到资产与威胁和脆弱性之间的联系,深入理解风险评估的意义。

5. 脆弱性分类的设计

信息系统或资产存在的脆弱性一般可以分为脆弱性类型、识别对象、识别内容三个方面。通过对此三个方面的选择可确定具体的脆弱性。

5.4.4　工具及资料

1. 漏洞扫描工具

绝大部分评估项目中,都会使用到漏洞扫描工具。

在脆弱性识别活动中,使用漏洞扫描工具对被评估系统进行扫描,花费低、效果好、节省人力和时间。扫描工具与网络相对独立,并且安装运行简单,可以避免仅靠人工方式来检查漏洞,是进行风险分析的有力工具。

在评估项目中,安全扫描主要是通过评估工具以本地扫描的方式对评估范围内的系统和网络进行扫描,从内部和外部(如在防火墙外)两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。

工具扫描活动,可以检测以下对象的安全漏洞:

(1) 信息探测类。

(2) 网络设备与防火墙。

(3) RPC 服务。

(4) Web 服务。

(5) CGI 问题。

(6) 文件服务。

(7) 域名服务。

(8) Mail 服务。

(9) Windows 远程访问。

(10) 数据库问题。

(11) 后门程序。

(12) 其他服务。

(13) 网络拒绝服务(DoS)。

(14) 其他问题。

从网络层次的角度来看，扫描活动可以覆盖如下三个层面的安全：系统层安全、网络层安全和应用层安全。

2. 各类检查列表

评估单位根据相关安全标准、最佳安全实践以及各自的经验积累，为各类评估实体对象设计的检查表用于手工识别信息系统中常见组件中存在的安全漏洞。

除了可以规避扫描工具引入的风险外，依靠检查列表进行手工的脆弱性识别，还可以识别那些工具不易检测到的安全漏洞或薄弱设置。

3. 渗透测试

渗透测试是指在获取用户授权后，通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现而利用的安全测试方法。这种测试方法可以非常有效地发现安全隐患，尤其是与代码审计相比，其使用的时间更短，也更有效率。在测试过程中，用户可以选择渗透测试的强度，例如，不允许测试人员对某些服务器或在线应用进行测试，防止影响其正常运行。通过对某些重点服务器进行准确、全面的测试，可以发现系统最脆弱的环节，以便对危害性严重的漏洞及时修补，以免后患。

进行渗透测试活动应在业务应用空闲的时候，或者在搭建的系统测试环境中进行。另外，渗透测试中采用的测试工具和攻击手段应在可控范围内，并同时准备完善的系统恢复方案。

建议选用技术水平高、有经验和具有良好职业道德的测试人员进行渗透性测试，这样才能达到良好的测试效果。

5.4.5 输出结果

1. 原始的识别结果

原始漏洞检测、识别报告文件。

2. 漏洞分析报告

对漏洞识别结果进行汇总、分析、分类，有助于被评估组织的信息安全主管或高层领导了解当前信息系统的安全状况，报告的原始数据可能来源于漏洞扫描的结果，也可能来源于漏洞扫描和手工检查的结果。

5.5 已有安全措施确认

5.5.1 工作内容

已有安全控制措施的识别与确认包括以下两个方面：技术控制措施的识别与确认，是识别已有的技术控制措施，并对其有效性进行分析和确认；管理和操作控制措施的识别与确认，是识别已有的管理和操作控制措施，并对其有效性进行分析和确认。

5.5.2　参与人员

本部分具体活动与参与人员的对应关系见表 5-11。

表 5-11　安全控制措施识别与确认工作的参与人员

序号	活动名称	参与人员	
		来自于评估单位	来自于被评估单位
1	技术控制措施的识别与确认	项目负责人 安全控制措施识别小组	项目负责人 识别活动中配合人员或访谈对象，主要包括被评估组织的安全主管、负责安全的管理员
2	管理和操作控制措施的识别与确认	项目负责人 安全控制措施识别小组	项目负责人 被评估组织的安全主管

5.5.3　工作方式

1. 技术控制措施的识别与确认

1）识别活动

技术安全控制措施一般会随着信息系统建立、运行和维护，不断建设和完善，其保护对象一般十分明确，所以识别的工作比较简单。例如，通过查看被评估组织最新的网络拓扑图，可以识别被评估组织目前已有的网络安全技术控制措施；配合人员访谈方式，便可以更详细地了解技术控制措施。

为了便于识别工作开展，建议安全控制措施识别小组按照信息系统的层次进行识别活动，如按照以下层次进行。

网络层：关注在网络层面上的安全技术控制措施，比如 FW/VPN、NIDS、安全网关、加密机等。

系统层：关注在系统层面上的安全技术控制措施，一般主要用于保护特定的系统，比如，防毒软件、HIDS、补丁分发工具等。

应用层：关注于专门针对应用或应用自身所固有的安全控制措施，例如，用于特定应用的 CA/PKI 设施、特定应用的审计功能。

数据层：关注于专门用于数据防护的安全控制措施，例如一致性校验、存储和备份系统。

上述分层识别的方式比较直观，但在识别每一个层面的安全技术控制措施时，还是难免发生遗漏。所以可以针对每个层面，从不同安全服务或功能入手，识别已有技术控制措施。

识别结束后，应按照一定的格式记录识别结果。记录已有技术控制措施时，应注明每项技术控制措施的目的、型号、所在位置和防护范围等。另外，通过访谈、分析，安全控制措施识别小组应提出缺失的技术控制措施及理由。

2）确认有效性

确认已有安全控制措施的有效性，是指检查控制措施是否达到了被评估组织的期望。

确定安全技术控制措施的有效性方式多种多样，其中主要的有访谈和调查、工作原理分析、无害测试三种。

2. 管理和操作控制措施的识别与确认

对于管理和操作方面的安全控制措施的识别和有效性确认活动，可以对照根据有关信息安全管理标准(ISO/IEC 27001)或最佳安全实践(NIST 的有关手册)制定的评估表格进行。本活动采用的具体工作方式主要是访谈和调查。识别小组在推动安全管理和操作控制措施识别和确认工作时，应按照如下工作流程进行：制定评估表格；确定访谈对象；访谈与调查。

3. 分析与统计

识别小组成员对调查结果进行统计和展现，便于被评估组织的高层能够从全局了解当前的安全管理状况。

根据统计结果，识别小组应结合被评估组织的实际情况，明确指明安全管理的哪些具体方面急需加强。已有控制措施的赋值如表 5-12 所示。

表 5-12　安全控制措施级别

已有控制措施值	定　义
0	没有相应的控制措施
50%	有相应的控制措施但不够完善或未得到很好的实施
100%	有相应的控制措施且比较完善，并得到很好的实施

5.5.4 工具及资料

安全控制措施识别与确认活动，需要用到以下工具或表格。

《技术控制措施调查表》：用于调查和记录被评估组织已经部署的安全控制措施。

《管理和操作控制措施调查表》：对照安全管理标准，调查和记录被评估组织已经采取的安全管理和操作控制措施。

涉密信息系统评测表格(可选，针对涉密信息系统的评估)：一般用于涉密信息系统的检查和评估，或一些重要信息系统的安全评估，如银行系统可以参考使用。

符合性检查工具：用于检查被评估组织当前对安全标准或策略的符合程度。

5.5.5 输出结果

安全控制措施识别与确认过程应提交以下输出结果：技术控制措施识别和确认结果；管理和操作控制措施识别和确认结果。

技术控制措施识别和确认结果包括：已有安全技术体系的描述，各项技术控制措施有效性分析结果，缺失或薄弱的安全控制措施的列表等。

管理和操作控制措施识别和确认结果包括：已有安全管理和操作控制措施的调查结果及其统计和分析结果，已有安全管理和操作控制措施的有效性检查结果，缺失或已经失效的

安全管理和操作控制措施情况等。

5.6　风险分析

在完成了资产识别、威胁识别、脆弱性识别，以及已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险。本标准给出了风险计算原理，以下面的范式形式化加以说明：

$$风险值 = R(A,T,V) = R(L(T,V),F(\mathrm{Ia},\mathrm{Va}))$$

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性；Ia 表示安全事件所作用的资产价值；Va 表示脆弱性严重程度；L 表示威胁利用资产的脆弱性导致安全事件的可能性；F 表示安全事件发生后造成的损失。风险计算包括以下三个关键计算环节：

1．计算安全事件发生的可能性

根据威胁出现频率及脆弱性的状况，计算威胁利用脆弱性导致安全事件发生的可能性，即：

$$安全事件的可能性 = L(威胁出现频率,脆弱性) = L(T,V)$$

在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）、资产吸引力等因素来判断安全事件发生的可能性。

2．计算安全事件发生后造成的损失

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的损失，即：

$$安全事件造成的损失 = F(资产价值,脆弱性严重程度) = F(\mathrm{Ia},\mathrm{Va})$$

部分安全事件的发生造成的损失不仅是针对该资产本身，还可能影响业务的连续性；不同安全事件的发生对组织的影响也是不一样的。在计算某个安全事件的损失时，应将对组织的影响也考虑在内。

部分安全事件造成的损失的判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件，例如，处于非地震带的地震威胁、在采取完备供电措施状况下的电力故障威胁等，可以不计算其损失。

3．计算风险值

根据计算出的安全事件的可能性以及安全事件造成的损失，计算风险值，即：

$$风险值 = R(安全事件的可能性,安全事件造成的损失) = R(L(T,V),F(\mathrm{Ia},\mathrm{Va}))$$

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成安全事件的可能性与安全事件造成的损失之间的二维关系；相乘法通过构造经验函数，将安全事件的可能性与安全事件造成的损失进行运算得到风险值。

目前通用的风险评估中风险值计算涉及的风险要素一般为资产、威胁、脆弱性；由威胁和脆弱性确定安全事件发生可能性，由资产和脆弱性确定安全事件的损失，以及由安全事件发生的可能性和安全事件的损失确定风险值。目前，常用的计算方法是矩阵法和相乘法。

GB/T 20984—2007 附录 A 中有矩阵法和相乘法的风险计算示例。

1）风险计算：相乘法

相乘法主要用于两个或多个要素值确定一个要素值的情形。即 $z=f(x,y)$，函数 f 可以采用相乘法。

相乘法的原理是：

$z=f(x,y)=x\odot y$。

当 f 为增量函数时，$\odot$ 可以为直接相乘，也可以为相乘后取模等，例如：

$z=f(x,y)=x\times y$，或 $z=f(x,y)=\sqrt{x\times y}$ 等。

相乘法提供一种定量的计算方法，直接使用两个要素值进行相乘得到另一个要素的值。相乘法的特点是简单明确，直接按照统一公式计算，即可得到所需结果。

共有两个重要资产，资产 A1 和资产 A2。

资产 A1 面临三个主要威胁，威胁 T1、威胁 T2 和威胁 T3；

资产 A2 面临两个主要威胁，威胁 T4 和 T5。

威胁 T1 可以利用资产 A1 存在的一个脆弱性，脆弱性 V1。

威胁 T2 可以利用资产 A1 存在的两个脆弱性，脆弱性 V2 和脆弱性 V3。

威胁 T3 可以利用资产 A1 存在的一个脆弱性，脆弱性 V4。

威胁 T4 可以利用资产 A2 存在的一个脆弱性，脆弱性 V5。

威胁 T5 可以利用资产 A2 存在的一个脆弱性，脆弱性 V6。

资产价值分别是：资产 A1＝4，资产 A2＝5。

威胁发生频率分别是：威胁 T1＝1，威胁 T2＝5，威胁 T3＝4，威胁 T4＝3，威胁 T5＝4。

脆弱性严重程度分别是：脆弱性 V1＝3，脆弱性 V2＝1，脆弱性 V3＝5，脆弱性 V4＝4，脆弱性 V5＝4，脆弱性 V6＝3。

相乘法风险计算过程：

两个资产的风险值计算过程类似，下面以资产 A1 为例使用相乘法计算风险值。

资产 A1 面临的主要威胁包括威胁 T1、威胁 T2 和威胁 T3，威胁 T1 可以利用的资产 A1 存在的脆弱性有一个，威胁 T2 可以利用的资产 A1 存在的脆弱性有两个，威胁 T3 可以利用的资产 A1 存在的脆弱性有一个，则资产 A1 存在的风险值包括 4 个。4 个风险值的计算过程类似，下面以资产 A1 面临的威胁 T1 可以利用的脆弱性 V1 为例，计算安全风险值。其中计算公式使用：

$z=f(x,y)=\sqrt{x\times y}$，并对 z 的计算值四舍五入取整得到最终结果。

(1) 计算安全事件发生可能性

威胁发生频率：威胁 T1＝1。

脆弱性严重程度：脆弱性 V1＝3。

计算安全事件发生可能性，安全事件发生可能性＝$\sqrt{1\times 3}=\sqrt{3}$。

(2) 计算安全事件的损失

资产价值：资产 A1＝4。

脆弱性严重程度：脆弱性 V1＝3。

计算安全事件的损失，安全事件损失＝$\sqrt{3\times4}=\sqrt{12}$。

(3) 计算风险值

安全事件发生可能性＝$\sqrt{3}$。

安全事件损失＝$\sqrt{12}$。

安全事件风险值＝$\sqrt{3}\times\sqrt{12}=6$。

按照上述方法进行计算，得到资产 A1 的其他的风险值，以及资产 A2 和资产 A3 的风险值。然后再进行风险结果等级判定。

(4) 结果判定

为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。可将风险划分为 5 级，等级越高，风险越高。

评估者应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。

表 5-13 提供了一种风险等级划分方法。

表 5-13　风险等级划分表

等级	标识	描　述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏，严重影响组织的正常经营，经济损失重大，社会影响恶劣
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

结果判定：确定风险等级划分如表 5-14 所示。

表 5-14　风险等级划分

风险值	1～5	6～10	11～15	16～20	21～25
风险等级	1	2	3	4	5

根据上述计算方法，以此类推，得到两个重要资产的风险值，并根据风险等级划分表，确定风险等级，如表 5-15 所示。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如，由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值，因此相乘法在风险分析中得到广泛采用。

表 5-15 风险结果

资 产	威 胁	脆 弱 性	风 险 值	风 险 等 级
资产 A1	威胁 T1	脆弱性 V1	6	2
	威胁 T2	脆弱性 V2	4	1
	威胁 T2	脆弱性 V3	22	5
	威胁 T3	脆弱性 V4	16	4
资产 A2	威胁 T4	脆弱性 V5	15	3
	威胁 T5	脆弱性 V6	13	3

2）风险计算：矩阵法

矩阵法主要适用于由两个要素值确定一个要素值的情形。首先需要确定二维计算矩阵，矩阵内各个要素的值根据具体情况和函数递增情况采用数学方法确定，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果。

即 $z=f(x,y)$，函数 f 可以采用矩阵法。

矩阵法的原理是：

$$x=\{x_1,x_2,\cdots,x_i,\cdots,x_m\},\quad 1\leqslant i\leqslant m, x_i \text{ 为正整数}$$

$$y=\{y_1,y_2,\cdots,y_j,\cdots,y_n\},\quad 1\leqslant j\leqslant n, y_j \text{ 为正整数}$$

以要素 x 和要素 y 的取值构建一个二维矩阵，如表 5-16 所示。矩阵行值为要素 y 的所有取值，矩阵列值为要素 x 的所有取值。矩阵内 $m\times n$ 个值即为要素 z 的取值，$z=\{z_{11},z_{12},\cdots,z_{ij},\cdots,z_{mn}\}$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$，$z_{ij}$ 为正整数。

表 5-16 矩阵构造

	y	y_1	y_2	…	y_j	…	y_n
X	x_1	z_{11}	z_{12}	…	z_{1j}	…	z_{1n}
	x_2	z_{21}	z_{22}	…	z_{2j}	…	z_{2n}
	…	…	…	…	…	…	…
	x_i	z_{i1}	z_{i2}	…	z_{ij}	…	z_{in}
	…	…	…	…	…	…	…
	x_m	z_{m1}	z_{m2}	…	z_{mj}	…	z_{mn}

对于 z_{ij} 的计算，可以采取以下计算公式：

$$z_{ij}=x_i+y_j$$

或

$$z_{ij}=x_i\times y_j$$

或

$$z_{ij}=\alpha\times x_i+\beta\times y_j$$

其中 α 和 β 为正常数。

z_{ij} 的计算需要根据实际情况确定，矩阵内 z_{ij} 值的计算不一定遵循统一的计算公式，但必须具有统一的增减趋势，即如果 f 是递增函数，z_{ij} 值应随着 x_i 与 y_j 的值递增，反之亦然。

矩阵法和相乘法计算过程基本相同。

共有三个重要资产，资产 A1、资产 A2 和资产 A3。

资产 A1 面临两个主要威胁,威胁 T1 和威胁 T2;
资产 A2 面临一个主要威胁,威胁 T3;
资产 A3 面临两个主要威胁,威胁 T4 和 T5。
威胁 T1 可以利用资产 A1 存在的两个脆弱性,脆弱性 V1 和脆弱性 V2;
威胁 T2 可以利用资产 A1 存在的三个脆弱性,脆弱性 V3、脆弱性 V4 和脆弱性 V5;
威胁 T3 可以利用资产 A2 存在的两个脆弱性,脆弱性 V6 和脆弱性 V7;
威胁 T4 可以利用资产 A3 存在的一个脆弱性,脆弱性 V8;
威胁 T5 可以利用资产 A3 存在的一个脆弱性,脆弱性 V9。
资产价值分别是:资产 A1=2,资产 A2=3,资产 A3=5。
威胁发生频率分别是:威胁 T1=2,威胁 T2=1,威胁 T3=2,威胁 T4=5,威胁 T5=4。
脆弱性严重程度分别是:脆弱性 V1=2,脆弱性 V2=3,脆弱性 V3=1,脆弱性 V4=4,脆弱性 V5=2,脆弱性 V6=4,脆弱性 V7=2,脆弱性 V8=3,脆弱性 V9=5。
(1) 计算安全事件发生可能性
威胁发生频率:威胁 T1=2。
脆弱性严重程度:脆弱性 V1=2。
首先构建安全事件发生可能性矩阵,如表 5-17 所示。

表 5-17 安全事件可能性矩阵

	脆弱性严重程度	1	2	3	4	5
威胁发生频率	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

然后根据威胁发生频率值和脆弱性严重程度值在矩阵中进行对照,确定安全事件发生可能性值等于 6。

由于安全事件发生可能性将参与风险事件值的计算,为了构建风险矩阵,对上述计算得到的安全风险事件发生可能性进行等级划分,如表 5-18 所示,安全事件发生可能性等级等于 2。

表 5-18 安全事件可能性等级划分

安全事件发生可能性值	1~5	6~11	12~16	17~21	22~25
发生可能性等级	1	2	3	4	5

(2) 计算安全事件的损失
资产价值:资产 A1=2。
脆弱性严重程度:脆弱性 V1=2。
首先构建安全事件损失矩阵,如表 5-19 所示。
然后根据资产价值和脆弱性严重程度值在矩阵中进行对照,确定安全事件损失值等于 5。

由于安全事件损失将参与风险事件值的计算,为了构建风险矩阵,对上述计算得到的安全事件损失进行等级划分。如表 5-20 所示,安全事件损失等级等于 1。

表 5-19 安全事件损失矩阵

	脆弱性严重程度	1	2	3	4	5
资产价值	1	2	4	6	10	13
	2	3	5	9	12	16
	3	4	7	11	15	20
	4	5	8	14	19	22
	5	6	10	16	21	25

表 5-20 安全事件损失等级划分

安全事件损失值	1～5	6～10	11～15	16～20	21～25
安全事件损失等级	1	2	3	4	5

（3）计算风险值

安全事件发生可能性＝2；安全事件损失等级＝1。

首先构建风险矩阵，如表 5-21 所示。

表 5-21 风险矩阵

	可能性	1	2	3	4	5
损失等级	1	3	6	9	12	16
	2	5	8	11	15	18
	3	6	9	13	17	21
	4	7	11	16	20	23
	5	9	14	20	23	25

然后根据安全事件发生可能性和安全事件损失在矩阵中进行对照，确定安全事件风险等于 6。

按照上述方法进行计算，得到资产 A1 的其他的风险值，以及资产 A2 和资产 A3 的风险。然后再进行风险结果等级判定。

（4）结果判定

风险等级划分方法见表 5-13。确定风险等级划分如表 5-22 所示。

表 5-22 风险等级划分

风险值	1～6	7～12	13～18	19～23	24～25
风险等级	1	2	3	4	5

根据上述计算方法，并根据风险等级划分表，确定风险等级，如表 5-23 所示。

矩阵法的特点在于通过构造两两要素计算矩阵，可以清晰罗列要素的变化趋势，具备良好的灵活性。在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，同时需要整体掌握风险值的确定，因此矩阵法在风险分析中同样得到广泛采用。

表 5-23　风险结果

资　　产	威　　胁	脆　弱　性	风　险　值	风 险 等 级
资产 A1	威胁 T1	脆弱性 V1	6	1
	威胁 T1	脆弱性 V2	8	2
	威胁 T2	脆弱性 V3	3	1
	威胁 T2	脆弱性 V4	9	2
	威胁 T2	脆弱性 V5	3	1
资产 A2	威胁 T3	脆弱性 V6	11	2
	威胁 T3	脆弱性 V7	8	2
资产 A3	威胁 T4	脆弱性 V8	20	4
	威胁 T5	脆弱性 V9	25	5

5.7　风险处理计划

通过风险评估的结果，加上组织的业务和法律法规对信息安全的要求，组织就可以得到总的安全需求。为满足总的安全需求，可以通过如图 5-1 和图 5-2 所示流程与方法进行风险管理。

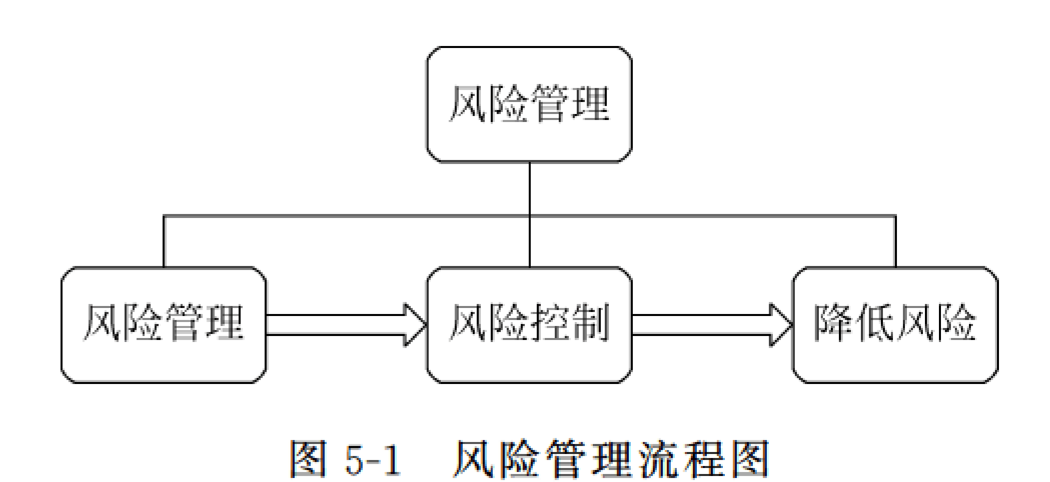


图 5-1　风险管理流程图

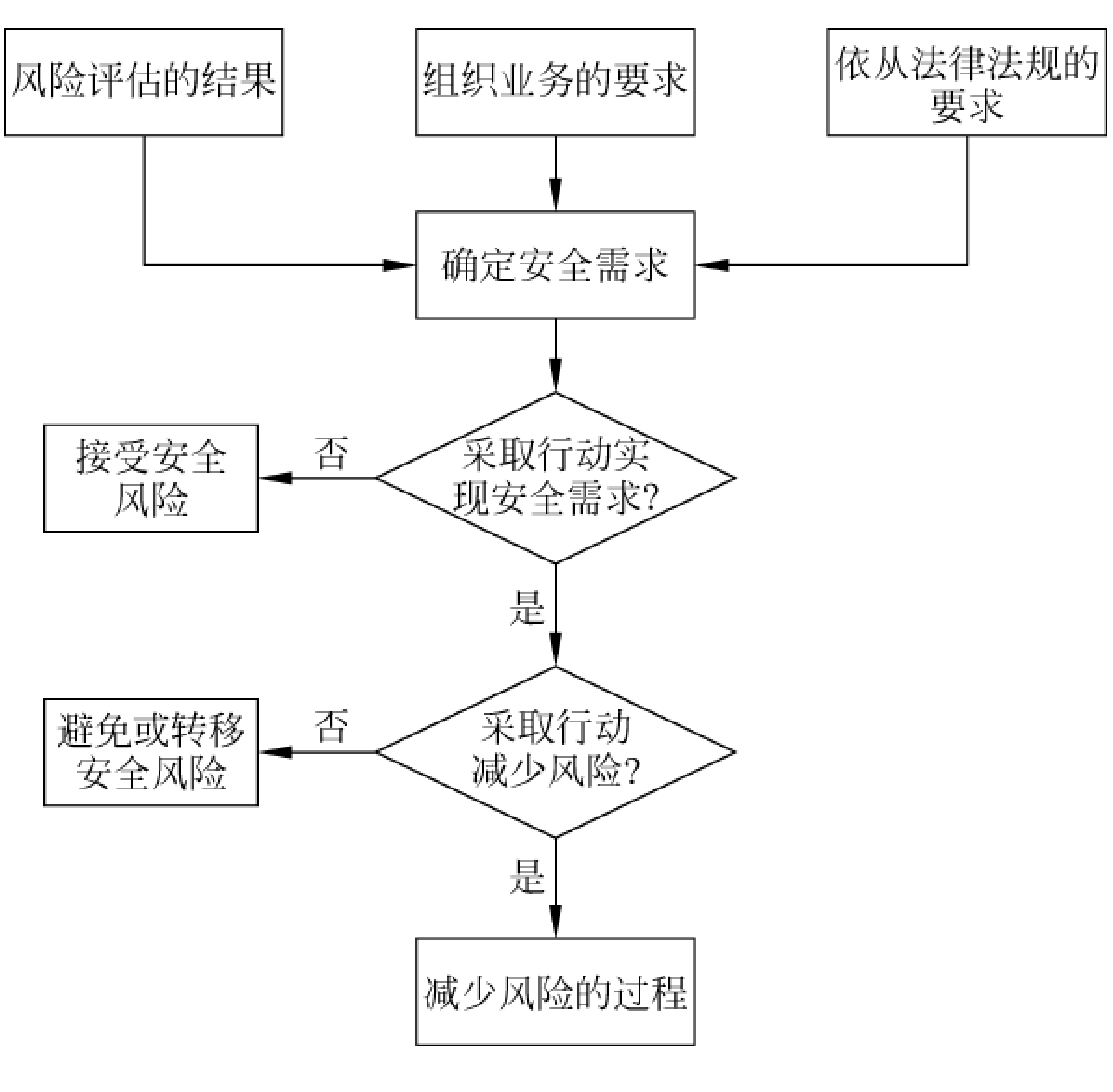


图 5-2　风险管理方法图

5.7.1 现存风险判断

依据信息安全风险评估结果，确定系统可接受的风险等级，把信息安全风险评估得出的风险等级划分为可接受和不可接受两种，形成风险接受等级划分表，表 5-24 是一种风险接受等级划分表的示例。

表 5-24 风险接受等级划分表示例

资 产 编 号	资 产 名 称	风 险 等 级	风险接受等级

5.7.2 控制目标确定

1. 风险控制需求分析

根据信息安全方针与策略的要求，为保护信息资产，管理层需要做出决策，对某些重要风险采取降低风险的办法，那么就需要导入合适的过程来选择相应的控制措施，通过选择和实施 ISO/IEC 27001 标准中的控制目标与控制措施，可以通过各种不同的方式来满足这些安全需求。

按照系统的风险等级接受程度，通过对信息系统技术层面的安全功能、组织层面的安全控制和管理层面的安全对策进行分析描述，形成已有安全措施的需求分析结果，表 5-25 是一种风险控制需求分析表的示例。

表 5-25 风险控制需求分析表示例

编 号	控 制 需 求	说 明

2. 风险控制目标

控制目标的确定和控制措施的选择原则要考虑风险平衡与成本效益的原则，而且要考虑信息安全是一个动态的系统工程，组织应及时对选择的控制目标和控制措施加以校验和调整，以适应变化了的情况，使组织的信息资产得到有效、经济、合理的保护。

ISO/IEC 27001 标准中的控制并不是无所不包的，组织需要考虑额外的控制目标和控制来适应其特殊的需要。另一方面，ISO/IEC 27001 的控制不是在任何情况下都必须使用，不能解释所有的环境和技术限制，也不能以适应所有潜在用户的方式进行提交。所以组织需要检查这些控制，选择他们自己必需的控制。用户根据实际情况，可以不使用其中的某些控制，或增加其中没有涉及的控制，这些需要在适用性声明中加以说明。

依据风险接受等级划分表、风险控制需求分析表，确定风险控制目标，表 5-26 是一种控制目标表的示例。

表 5-26　控制目标表示例

编　　号	控 制 目 标	说　　明

5.7.3　控制措施选择

依据风险控制需求分析表、控制目标表，制定控制措施的优先级别，控制措施的优先级定义参见表 5-27。

表 5-27　控制措施优先级表示例

控制措施优先级	定　　义
高	控制成本低和/或对控制目标的安全状况影响大，建议优先落实
中	控制成本较低和/或对控制目标的安全状况影响较大，在短时间内落实
低	控制成本高和/或对控制目标的安全状况影响较低，在一定时间内落实

针对控制目标，综合考虑控制成本和实际的风险控制需求，建议采取适当的控制措施，表 5-28 是一种安全控制措施选择表的示例。

表 5-28　安全控制措施选择表示例

编　　号	控 制 措 施	对应控制目标	优　先　级

为了识别风险，要综合考虑威胁、脆弱性及其他风险评估的结果；一旦风险被识别出来后，下一步要做的工作就是选择控制措施减少风险，即通过以下途径达到降低风险的目的，几种风险管理方法描述如下：

1. 接受风险

第一种方法就是决定是否在这一点上接受风险，不做任何事情，不引入控制措施。如果认为风险是组织不能接受的，那么就需要考虑其他三种方法来应对某个风险或某些风险。

2. 避免风险

避免风险，又称为规避风险，是组织决定绕过风险。例如，将重要的计算机系统与 Internet 隔离，免受外部网络的攻击。把整个组织撤离到安全场合可能会需要巨大的投入，这时可以考虑采用风险转移的方式；尽管有黑客的威胁，由于有业务的需要，组织不可避免地要使用 Internet，这时可以考虑降低风险的方式。采用避免风险的措施时，需要在业务需求与资金投入方面进行权衡。

3. 转移风险

转移风险是组织在无法避免风险时的一种可能的选择，或者是在减少风险很困难，成本很高时，组织采取的一种方法。例如，对已评估确认的价值较高，风险较大的资产进行保险，通过购买商业保险将风险进行转移，或将高风险的信息处理业务外包给第三方。

4. 降低风险

所谓降低风险就是通过选择控制目标与控制措施来降低评估确定的风险。需要结合下列各种控制措施来降低风险，使风险达到可接受的安全水平，减少危险、减少脆弱性、减少可能的影响、检测意外事件、响应并恢复。例如，通过安装防病毒软件，防止系统受病毒感染；系统经常性地安装补丁包，修补系统漏洞，以防止系统脆弱性被利用；建立业务持续性计划，把灾难造成的损失降到最低；使用网络管理系统，网络性能与故障进行监测，及时发现出现的问题。

选择哪一种减少风险的方式，要根据组织运营的具体业务环境与条件来决定，总的原则是及时为减少风险所选的控制要与特定的业务要求相匹配，而且要对所选的控制进行充分的评估。

5. 处置残留风险

组织在实施所选择的控制措施后，总是有残留风险，这是因为组织的信息系统不可能是绝对安全的。甚至有些残留风险是组织有意对某些资产没有进行保护而造成的，这是由于风险较低或要实施安全控制的成本太高。

风险接受是一个对残留风险进行确认和评价的过程。在安全控制实施后，组织就对已实施的安全控制进行评审，即对所选择的控制措施在多大程度上降低了风险做出判断，并根据残留风险的大小，将残留风险分为“可接受的”或“不可接受”的风险。对于无法接受的风险不应该容忍，而应该考虑再增加控制以降低那些风险。对于每一个无法接受的风险，必须将风险降低到一个可接受的水平。

组织的信息系统绝对安全(即零风险)是不可能的。组织在实施选择的控制后，总是有残留的风险，称为残留风险或残余风险。为确保组织的信息安全，残余风险应在可接受的范围内。一般情况下，

$$残余风险\ Rr = 原有风险\ Ro - 控制风险\ Rx$$

$$残余风险\ Rr \leqslant 可接受风险\ Rt$$

组织在完成了风险评估、降低风险与接受风险的风险管理过程后，可以将风险控制在一个可以接受的水平，但这并不意味着风险评估工作的结束。事实上，随着时间的推移，由于组织的业务环境在不断变化，新的威胁与脆弱性也在不断增加，组织由于业务要求可能要增加新的信息处理设施，有关信息的法律法规也在变化，所以风险也是随时间而变化的，风险管理是动态的、持续改进的过程，组织需要进行动态的风险评估与风险管理。特别是在以下情况发生时，应进行临时的风险评估，以便及时识别风险并进行有效控制：

(1) 当新增信息资产时。

(2) 当系统发生重大变更时。

（3）发生严重信息安全事故时。
（4）组织认为有必要时。

5.8 风险评估报告

通过信息安全风险评估，风险评估小组对组织的风险状况有一个非常清晰的理解，有关风险状况的信息必须以清晰有效的方式传达给组织。因此，需要编写记录评估过程所得结果的风险评估报告，供高层管理人员审阅，高层管理人员据此报告决定控制措施的选择和风险接受等问题。表 5-29 给出了一个信息安全风险评估报告的示例。

表 5-29 信息安全风险评估报告示例

封皮	XXXX 信息安全风险评估报告 被评估的系统： 被评估单位： 评估类别： 负责人： 评估时间：
目录	
第 1 章 介绍评估准备的相关内容。	综述
第 2 章 介绍资产的识别和评价结果。	识别并评价资产
第 3 章 介绍威胁的识别和评价结果。	识别并评估威胁
第 4 章 介绍脆弱性的识别和评价结果。	识别并评估脆弱性
第 5 章 介绍已有安全措施的识别和分析结果。	识别安全措施
第 6 章 介绍可能性和影响的分析结果。	分析可能性和影响
第 7 章 介绍风险的计算结果。	风险计算
第 8 章 介绍需控制的风险及控制措施。	风险控制
第 9 章 对本次评估进行总结。	总结

思考题

1. 简单叙述风险评估准备阶段的主要工作内容。
2. 简单叙述资产识别的工作内容和工作方式。
3. 简单叙述威胁识别的工作内容和参与人员。
4. 叙述针对潜在威胁的识别活动的主要内容。
5. 如何构建威胁场景?
6. 简单叙述脆弱性识别的工作方式。
7. 叙述风险计算原理。

第6章 信息系统生命周期各阶段的风险评估

信息安全风险评估应贯穿于信息系统的整个生命周期的各阶段中。信息系统生命周期是某一系统从无到有、再到废弃的整个过程，包括规划、设计、实施、运维和废弃5个基本阶段，各阶段中涉及的风险评估的原则和方法是一致的，但由于各阶段实施的内容、对象、安全需求不同，使得风险评估的对象、目的、要求等各方面也有所不同。

6.1 规划阶段的信息安全风险评估

在信息系统的规划阶段，确定信息系统的目的、范围和需求，分析和论证可行性，提出总体方案。

规划阶段信息安全风险评估的目的是识别系统的业务战略，用以支撑系统安全需求及安全战略等。规划阶段的评估应能够描述信息系统建成后对现有业务模式的作用，包括技术、管理等方面，并根据其作用确定系统建设应达到的安全目标。

本阶段评估中，资产、脆弱性不需要识别；威胁应根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行分析。评估着重以下几方面。

（1）是否依据相关规则，建立了与业务战略一致的信息系统安全规划，并得到最高管理者的认可。

（2）系统规划中是否明确信息系统开发的组织、业务变更的管理、开发优先级。

（3）系统规划中是否考虑信息系统的威胁、环境，并制定总体的安全方针。

（4）系统规划中是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等。

（5）系统规划中是否描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、组织安全政策、专门技术和知识等。

规划阶段的评估结果应体现在信息系统整体规划或项目建议书中。

6.2 设计阶段的信息安全风险评估

在信息系统的设计阶段：依据总体方案，设计信息系统的实现结构（包括功能划分、接口协议和性能指标等）和实施方案（包括实现技术、设备选型和系统集成等）。

本阶段风险评估中，应详细评估设计方案中对系统面临威胁的描述，将使用的具体设备、软件等资产及其安全功能需求列表。对设计方案的评估着重以下几方面进行：

(1) 设计方案是否符合系统建设规划，并得到最高管理者的认可。

(2) 设计方案是否对系统建设后面临的威胁进行了分析。重点分析来自物理环境和自然的威胁，以及由于内、外部入侵等造成的威胁。

(3) 设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析，制定信息系统的总体安全策略。

(4) 设计方案是否采取了一定的手段来应对系统可能的故障。

(5) 设计方案是否对设计原型中的技术实现以及人员、组织管理等各方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性。

(6) 设计方案是否考虑随着其他系统接入而可能产生的风险。

(7) 系统性能是否满足用户需求，并考虑到峰值的影响，是否在技术上考虑了满足系统性能要求的方法。

(8) 应用系统(含数据库)是否根据业务需要进行了安全设计。

(9) 设计方案是否根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型。

(10) 设计活动中所采用的安全控制措施、安全技术保障手段对风险结果的影响，在安全需求变更和设计变更后，也需要重复这项评估。

设计阶段的评估可以以安全建设方案评审的方式进行，判定方案提供安全功能与信息技术、安全技术标准的符合性。评估结果应体现在信息系统需求分析报告或建设实施方案中。

6.3 实施阶段的信息安全风险评估

在信息系统实施阶段，按照实施方案，购买和检测设备，开发定制功能集成、部署、配置和测试系统，培训人员等。

实施阶段信息安全风险评估的目的是根据系统安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的安全性能进行验证。根据设计阶段分析的威胁和建立的安全控制措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施，实施阶段应对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定安全措施能否抵御现有威胁、脆弱性的影响。实施阶段风险评估主要对系统的开发、技术、产品的获取与系统的交付实施两个过程进行评估。开发、技术、产品获取过程的评估要点包括以下几个。

(1) 法律、政策、适用标准和指导方针。直接或间接影响信息系统安全需求的特定法律；影响信息系统安全需求、产品选择的政府政策、国际或国家标准。

(2) 信息系统的功能需要：安全需求是否有效地支持系统的功能。

(3) 成本效益风险：是否根据信息系统的资产、威胁和脆弱性的分析结果，确定在符合相关法律、政策、标准和功能需要的前提下选择最合适的安全措施。

(4) 评估保证级别，是否明确系统建设后应进行怎样的测试和检查，从而确定是否满足

项目建设、实施规范的要求。

系统交付实施过程的评估要点包括：

(1) 根据实际建设的系统，详细分析资产、面临的威胁和脆弱性。

(2) 根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁。

(3) 评估是否建立了与整体安全策略一致的组织管理制度。

(4) 对系统实现的风险控制效果与预期设计的符合性进行判断，如存在较大的不符合，应重新进行信息系统安全策略的设计与调整。

本阶段的信息安全风险评估可以采取对照实施方案和标准要求的方式，对实际建设结果进行测试、分析。

6.4 运维阶段的信息安全风险评估

在信息系统的运行和维护阶段，保证信息系统在自身和所处环境的变化始终能正常工作和不断升级。

运维阶段信息安全风险评估是了解和控制运行过程中的信息系统安全风险较为全面的风险评估。评估内容包括对真实运行的信息系统、资产、威胁、脆弱性等各方面。

(1) 资产评估。在真实环境下较为细致的评估，包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等。本阶段资产识别是前期资产识别的补充与增加。

(2) 威胁评估。应全面地分析威胁的可能性和影响程度。对非故意威胁导致安全事件的评估可以参照安全事件的发生概率；对故意威胁导致安全事件的评估主要就威胁的各个影响因素做出专业判断。

(3) 脆弱性评估。全面的脆弱性评估，包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性评估。技术脆弱性评估可以采取核查、扫描、案例验证、渗透测试的方式实施；安全保障设备的脆弱性评估，应考虑安全功能的实现情况和安全保障设备本身的脆弱性。管理脆弱性评估可以采取文档、记录核查等方式进行验证。

(4) 风险计算。根据风险计算的相关方法，对重要资产的风险进行定性或定量的风险分析，描述不同资产的风险高低状况。

运维阶段的信息安全风险评估应定期执行；当组织的业务流程、系统状况发生重大变化时，也应进行风险评估。重大变更主要包括以下变更：

① 增加新的应用或应用发生较大的变更。

② 网络结构和连接状况发生较大的变更。

③ 技术平台大规模的更新。

④ 系统扩容或改造。

⑤ 发生重大安全事件后，或基于某些运行记录怀疑将发生重大安全事件。

⑥ 组织结构发生重大变动对系统产生影响。

6.5 废弃阶段的信息安全风险评估

当信息系统不能满足要求时，信息系统进入废弃阶段，对信息系统的过时或无用部分进行报废处理。根据废弃的程度，分为部分废弃和全部废弃两种。

废弃阶段信息安全风险评估着重在以下几个方面：

(1) 确保硬件或软件等资产及残留信息得到了适当的处置，并确保系统组件被合理地丢弃或更换。

(2) 如果被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接。还应考虑系统废弃后与其他系统的连接是否被关闭。

(3) 如果在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确保是否会增加风险或引入新的风险。

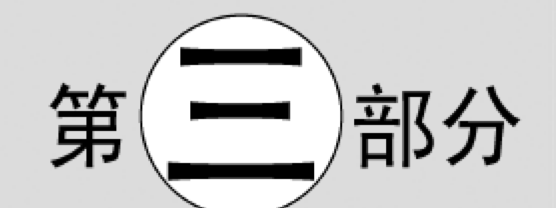
(4) 是否建立了流程，确保更新过程在一个安全、系统化的状态下完成。

本阶段应重点对废弃资产对组织的影响进行分析，并根据不同的影响制定不同的处理方式。对由于系统废弃可能带来的新的威胁进行分析，并改进新系统或管理模式。对废弃资产的处理过程应在有效的监督之下实施，同时对废弃的执行人员进行安全教育。

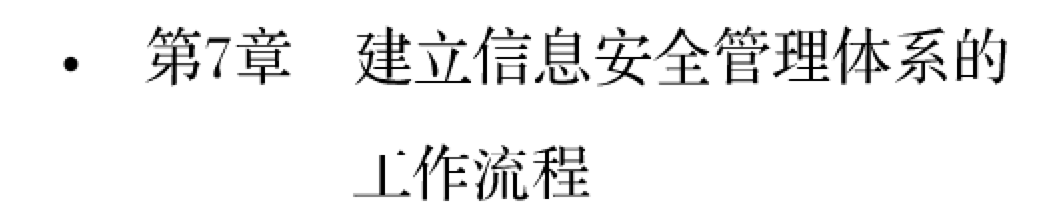
信息系统的维护工作的技术人员和管理人员均应该参与此阶段的评估。

思考题

1. 规划阶段的信息安全风险评估包括哪几方面的内容？
2. 简单叙述设计阶段信息安全风险评估的主要内容。
3. 系统交付实施过程的评估要点包括哪些内容？
4. 叙述运维阶段信息安全风险评估的主要内容。
5. 废弃阶段信息安全风险评估包括哪几个方面的内容？



信息安全管理



第7章 建立信息安全管理体系的工作流程

7.1 信息安全管理体系的策划与准备

7.1.1 信息安全管理体系

1. 信息安全管理体系的定义

信息安全管理体系(Information Security Management System,ISMS)是组织在整体或特定范围内建立的信息安全方针和目标,以及完成这些目标所用的方法和手段所构成的体系。它是信息安全管理活动的直接结果,表示为方针、原则、目标、方法、计划、活动、程序、过程和资源的集合。

ISO/IEC 27001是建立和维持信息安全管理体系的标准,标准要求组织通过确定信息安全管理体系范围,制定信息安全方针,明确管理职责,以风险评估为基础选择控制目标与控制措施等一系列活动来建立信息安全管理体系。信息安全管理体系一旦建立,组织应按体系的规定要求进行运作,保持体系运行的有效性。信息安全管理体系应形成一定的文件,即组织应建立并保持一个文件化的信息安全管理体系,其中应阐述被保护的资产、组织风险管理方法、控制目标与控制措施、信息资产需要保护的程度等内容。

2. 组织内部成功实施信息安全管理体系的关键因素

(1) 反映业务目标的安全方针、目标和活动。
(2) 与组织文化一致的、实施安全的方法。
(3) 来自管理层的有形支持与承诺。
(4) 对信息安全要求、风险评估和风险管理的良好理解。
(5) 向所有管理者及雇员推行信息安全意识。
(6) 向所有雇员和承包商分发有关信息安全方针和标准的导则。
(7) 提供适当的信息安全的培训与教育。
(8) 用于评价信息安全管理绩效及反馈改进建议,并有利于综合平衡的测量系统。

3. 建立信息安全管理体系的步骤

不同的组织在建立与完善信息安全管理体系时,可根据自己的特点和具体的情况,采取

不同的步骤和方法。但总体来说，建立信息安全管理体系一般要经过下列6个基本步骤：

(1) 信息安全管理体系的策划与准备。

(2) 信息安全管理体系文件的编制。

(3) 建立信息安全管理框架。

(4) 信息安全管理体系的运行。

(5) 信息安全管理体系的审核。

(6) 信息安全管理体系的管理评审。

7.1.2 信息安全管理体系的准备

1. 管理承诺

组织最高管理层应提供其承诺建立、实施、运行、监控、评审、维护和改进信息安全管理体系的证据，这是成功实施信息安全管理体系的重要保护，管理承诺包括：

(1) 建立信息安全方针。

(2) 建立信息安全目标和计划。

(3) 为信息安全确立角色和责任。

(4) 向组织传达信息安全目标和符合信息安全策略的重要性，组织的责任及持续改进的需要。

(5) 提供足够的资源以开发、实施、运行和维护信息安全管理体系。

(6) 确定可接受风险的水平。

(7) 进行信息安全管理体系的评审。

2. 组织与人员建设

为在组织中顺利建立信息安全管理体系，需要建立有效的信息安全机构，对组织中的各类人员分配角色、明确权限、落实责任并予以沟通。

1) 成立信息安全委员会

信息安全委员会由组织的最高管理层，及与信息安全管理有关的部门负责人、管理人员、技术人员组成，定期召开会议，就以下重要信息安全议题进行讨论并做出决策，为组织信息安全管理提供导向与支持：

(1) 评审和审批信息安全方针。

(2) 分配信息安全管理职责。

(3) 确认风险评估的结果。

(4) 对与信息安全管理有关的重大事项做出决策。

(5) 评审与监督信息安全事故。

(6) 审批与信息安全管理有关的其他重要事项。

2) 任命信息安全管理经理

组织最高管理者在管理层中指定一名信息安全管理经理，分管组织的信息安全事宜，具体有以下责任：

(1) 确定信息安全管理标准，建立、实施和维护信息安全管理体系。

（2）负责组织的信息安全方针与安全策略的贯彻与落实。

（3）向最高管理者提交信息安全管理体系绩效报告，以供评审信息安全管理体系提供证据。

（4）就信息安全管理的有关问题与外部各方面进行联络。

3）组建信息安全管理推进小组

在信息安全委员会的批准下，由信息安全管理经理组建信息安全管理推进小组并对其进行管理。小组成员要懂信息安全技术知识，有一定的信息安全管理技能，并且有较强的分析能力及文档编写能力，小组成员一般是企业各部门的骨干人员。

4）保证有关人员的作用、职责和权限得到有效沟通

用适当的方式，如通过培训、制定文件等方式，让每位员工明白自己的作用、职责与权限，以及与其他部分的关系，以保证全体员工各司其职，相互配合，有效地开展活动，为信息安全管理体系的建立做出贡献。

5）组织机构的设立原则

（1）合适的控制范围：例如，一般情况下，一个经理直接控制的下属管理人员不应超过10人。

（2）合适的管理层次：例如，公司负责人与基层管理部门之间的管理层数应保持最少程度。

（3）一个上级的原则。

（4）责、权、利一致的原则。

（5）既无重叠，又无空白的原则。

（6）执行部门与监督部门分离的原则。

（7）信息安全部门有一定的独立性，不应成为生产部门的下属单位。

6）信息安全管理体系组织结构设立及职责划分的注意事项

（1）如果现有的组织结构合理，则只需将信息安全标准的要求分配落实到现有的组织结构中即可；如果现有的组织结构不合理，则按上面5）中所述规则对组织结构进行调整。

（2）应将组织内的部门设置及各部门的信息安全职责、权限及相互关系以文件的形式加以规定。

（3）应将部门内岗位设置及各岗位的职责、权限和相互关系以文件的形式加以规定。

（4）日常的信息安全监督检查工作应有专门的部门负责。

（5）对于大型企业来说，可以设置专门的安全部，安全部设立首席安全执行官，首席安全执行官直接向组织最高管理层负责。

（6）对于小型企业来说，可以把信息安全管理工作划归到信息部或其他相关部门。

3．编制工作计划

建立信息安全管理体系是一个复杂的系统工程，它的建立需要半年甚至更长的时间，包括培训、风险评估、文件编写等大量工作。

为确保体系顺利建立，组织应进行统筹安排，即制定一个切实可行的工作计划，明确不同时间段的工作任务与目标及责任分工，控制工作进度，突出工作重点，例如以表7-1的形式安排总体计划。总体计划被批准后，可针对具体工作项目制定详细计划，例如文件编写计划。

在制定计划时，组织应考虑资源需求，例如人员需求、培训经费、办公设施、聘请咨询公

司的费用等。如果寻求体系的第三方认证，还要考虑认证的费用。组织最高管理层应确保提供建立体系所必需的人力与财务资源。信息安全管理体系总体工作计划，如表 7-1 所示。

表 7-1 信息安全管理体系总体工作计划

序号	阶段	项目	负责部门/人	日期
1	准备阶段	1）领导决策 • 做出实施 ISMS 的决策 • 成立信息安全管理委员会 • 任命信息安全管理经理	最高管理者	
		2）建立信息安全组织机构，并设计方案 • 设立信息安全管理推进小组 • 拟定 ISMS 实施草稿，并由信息安全管理委员会讨论通过	信息安全管理委员会；信息安全管理经理	
		3）编制 ISMS 工作计划 • 详细实施计划 • 认证计划 • 培训计划	信息安全管理经理；信息安全管理推进小组	
		4）学习培训	信息安全管理经理；人事部	
2	初始状态评审	5）初始状态评审 • 了解组织概况、业务类别、企业文化等基本情况，收集适用于组织的法律、法规和其他与信息安全相关的文件和数据 • 信息安全风险评估、选择风险控制措施 • 评估现有信息安全控制措施的适用性 • 评价现行管理体系与 ISO/IEC 27001 的差距	信息安全管理经理；信息安全管理推进小组	
3	体系设计	6）确定 ISMS 方针和目标	最高管理者	
		7）编制 ISMS 管理方案	推进小组；组织内相关部门	
		8）ISMS 责任分配及资源配备 • 必要时对组织结构进行调整 • 将各项 ISMS 活动责任分配落实到各职能部门，编制职能分配矩阵表 • 识别资源需求，配置必要的资源	最高管理者；信息安全管理经理	
4	文件编制	9）文件的总体设计 • 确定文件清单，确定 ISMS 文件与 ISO/IEC 27001 标准条款的对照表 • 制定文件编写计划 • 编写指导性文件	信息安全管理经理；推进小组	
		10）编写 ISMS 管理手册 • 编写；讨论修改；审核；批准	最高管理者；各部门经理；信息安全管理经理；推进小组	
		11）程序文件编写、配套表格设计 • 编写；讨论修改；审核；批准	各部门经理；信息安全管理经理；推进小组	
		12）作业指导书编写、配套表格设计 • 编写；讨论修改；审核；批准	相关业务人员；各部门经理；推进小组	

续表

序号	阶段	项　　目	负责部门/人	日期
5	实施运行	13）ISMS 文件的学习	各部门经理；信息安全管理经理	
		14）试运行前的准备 • 检查资源配置到位情况 • 制备各类标签、标识用品记录表格、表卡等 • 试运行前或试运行初最好把计量工作做好 • 宣传鼓动	信息安全管理经理；各部门经理	
		15）宣布试运行	最高管理者	
		16）贯彻实施、整改完善	各部门经理	
		17）内审员的培训	信息安全管理经理；人事部	
		18）ISMS 内部审核	内部审核小组	
		19）管理评审	最高管理者	
6	审核认证	20）申请认证	信息安全管理经理	
		21）认证	各部门经理	

4. 能力要求与教育培训

组织的管理体系通常是按照国际标准或国家标准的要求建立起来的，信息安全管理体系建立的依据是 ISO/IEC 27001 信息安全管理体系规范标准。为了强化组织信息安全的意识，明确信息安全管理体系的基本要求，进行信息安全管理体系标准的培训是十分必要的和必须的，这也是组织搞好信息安全管理的关键因素之一。

培训工作要分层次、分阶段、循序渐进地进行，而且必须是全员培训。分层次培训是指对不同层次的人员开展有针对性的培训，这包括对决策层、管理层、审核验证人员及操作执行人员的培训，而且培训的内容也各有侧重；分阶段是指在信息安全管理体系的建立、实施与保持的不同阶段，培训工作要有计划地安排实施，如在体系建立初期对管理层的宣传贯彻培训、在风险评估前对评估人员所进行的风险评估方法的培训等；培训可以采用外部与内部相结合的方式。

对从事信息安全管理工作的人员，应具有相应的能力要求，在教育经历方面，组织应对其能力做出适当的规定。有以下要点：

（1）组织应对人员的培训、意识和能力的要求建立文件化的程序。

（2）人员能力的基本要求：

① 适当的教育程度，通常是指为从事不同的、对信息安全有影响的工作所需的最低学历教育。

② 适当的培训，通常是指为从事某一岗位工作之前需接受的培训，例如对内审员的培训要求。

③ 适当的经历，通常是指为了更有效地完成工作任务所需的工作经验和专业技能。

（3）保证人员能力的措施：

① 根据任职条件、法律、法规要求、组织发展的需要，识别人员能力的需求。

② 提供培训或采取其他措施满足对人员的能力需求。

③ 评价所采取措施的有效性，评价方式有考核、业绩评定、管理人员评价、观察等。

（4）培训的实施：

① 确定培训需求。

② 制定培训计划。

③ 实施培训。

④ 培训后考核。

⑤ 培训结果的处理。

⑥ 记录保存。

（5）培训的内容：

① 信息安全知识、安全技能培训，实际操作技能考核等。

② 向所有管理者及雇员进行安全意识的培训。

③ 有关信息安全的法律、法规、制度的培训。

④ 向所有雇员和承包商培训有关信息安全政策和标准。

⑤ 书面的安全方针、策略、规程、作业指导书。

（6）培训的方式：

① 内部培训、外部培训、实习、自学考试、学术交流。

② 采用不同媒体来宣传信息安全，如公司邮件、网页。

③ 安全规则的可视化执行。

④ 模拟安全事故以改善安全规程。

⑤ 员工签订保密协议，了解安全需求。

7.2 信息安全管理体系的设计与建立

7.2.1 编写信息安全管理体系文件

1. ISMS 文件

信息安全管理体系需要编写各种层次的信息安全体系文件，这是建立信息安全管理体系的重要基础性工作。文件应包括管理决策的记录，以确保措施可以追溯到管理决策和方针。重要的是要能够展示从选择的控制措施回溯到风险评估和风险处置过程因果的关系，最终回溯到 ISMS 方针和目标。ISMS 文件应包括：

（1）形成文件的 ISMS 方针与策略。

（2）ISMS 范围。

（3）ISMS 的支持性程序和控制。

（4）风险评估方法的描述。

（5）风险评估报告。

（6）风险处置计划。

（7）ISMS 的控制目标与控制措施。

（8）ISMS 管理和具体操作的过程。

（9）标准中所要求的记录。
（10）信息系统安全相关职责描述和相关的活动事项。
（11）适用性声明。

2. 文件的作用

从总体来看，文件的作用有：

1）阐述声明的作用

信息安全管理体系文件是客观地描述信息安全体系的法规性文件，为组织的全体人员了解信息安全管理体系创造了必要的条件。企业向客户或认证机构提供《信息安全管理手册》起到了对外声明的作用。

2）规定、指导的作用

信息安全管理体系文件规定了组织员工应该做什么、不应该做什么的行为准则，以及如何做的指导性意见，对员工的信息安全行为起到了规范、指导作用。

3）记录、证实的作用

信息安全管理记录具有记录和证实信息安全管理体系运行有效的作用。其他文件则具有证实信息安全管理体系客观存在和运行适用性的作用。

从评价和改进信息安全管理体系的角度来看，文件具有以下三种具体作用：
（1）评价信息安全管理体系的作用。
（2）保障信息安全改进的作用。
（3）平衡培训要求的作用。

3. 文件的层次

信息安全管理体系关于文件的描述中，没有强求将其形成专门的手册形式，也没有刻意要求组织将体系文件分成若干层次，但依据 ISO 9000 的成功经验，在具体实施中，为便于运作并具有操作性，建议把 ISMS 管理文件分成以下几个层次，即适用性声明、管理手册、程序文件、作业文件指导书、记录。

1）适用性声明

适用性声明是组织为满足安全需要而选择的控制目标和控制方式的评论性文件。在适用性声明文件中，应明确列出组织根据信息安全要求（包括风险评估、法律法规、业务三方面）从 ISO/IEC 27001 中选择的控制目标与控制方式，并说明选择与不选择的理由；如果有额外的控制目标与控制方式也需要一并说明。

2）ISMS 管理手册

ISMS 管理手册是阐明组织的 ISMS 方针，并描述其 ISMS 的文件。ISMS 手册至少包括以下内容：
（1）信息安全方针的阐述。
（2）信息安全管理的体系范围。
（3）信息安全策略的描述。
（4）控制目标与控制方式的描述。
（5）程序或其引用。

(6) 关于手册的评审、修改与控制的规定。

3) 程序文件

程序是为进行某项活动所规定的途径或方法。信息安全管理程序包括两部分：一部分是实施控制目标与控制方式的安全控制程序，另一部分是为覆盖信息安全管理体系的管理与运作的程序。程序文件应描述安全控制或管理的责任及相关活动，是信息安全政策的支持性文件，是有效实施信息安全政策、控制目标与控制方式的具体措施。

4) 作业指导书

作业指导书是程序文件的支持性文件，用以描述具体的岗位和工作现场如何完成某项工作任务的具体作法，包括作业指导书、规范、指南、图样、报告、表格等，例如设备维护规程或维护手册。作业指导性文件可以被程序文件所引用，对程序文件中整个程序或某些条款进行补充、细化。

5) 记录

记录作为信息安全管理体系运行结果的证据，是一种特殊的文件。组织在编写信息安全方针手册、程序文件及作业指导文件时，应根据安全控制与管理要求确定组织所需要的信息安全记录，组织可以通过利用现有的记录、修订现有的记录和增加新的记录三种方式来获得。记录可以是书面记录，也可以是电子媒体记录，每一种记录应进行标识，记录应有可追溯性。记录内容与格式应该符合组织业务运作的实际并反映活动结果，且方便记录人的使用。

4. 文件的编写

由于 ISMS 文件是信息安全管理体系的基础，组织应当建立恰当的程序对 ISMS 进行管理，在文件生命周期的各个阶段，如编写、审核、批准、发布、使用、保管、回收、销毁等，都需要有适宜的控制措施。

1) 文件编写的原则

(1) ISMS 文件层次清楚、结构合理。

(2) ISMS 文件应保持其相对的稳定性和连续性。

(3) ISMS 文件不是信息安全管理现状的简单写实，应随着 ISMS 的不断改进而完善。

(4) 编写 ISMS 文件时，要继承以往的有效经验与作法。

(5) 应发动各部门有实践经验的人员集思广益，共同参与。

(6) ISMS 文件应当可以作为组织 ISMS 有效运行并得到保持的客观证据，向相关方、第三方证实组织 ISMS 的运行情况。

(7) 文件的编制和形式应考虑企业的产品特点、规模、管理经验等。文件的详略程度应与人员的素质、技能和培训等因素相适宜。

2) 编写前的准备

(1) 指定编写主管机构，指导和协调文件的编写工作。

(2) 收集整理企业现有文件。

(3) 对编写人员进行培训，使之明确编写的要求、方法、原则和注意事项。

(4) 为了使 ISMS 文件统一协调，达到规范化和标准化的要求，应编写指导性文件，就文件的要求、内容、体例和格式做出规定。

3）编写的策划与组织

确定要编写的文件目录，制定编写计划，落实编写、审核、批准人员，拟定编写进度。

5. 文件的管理

1）文件控制

组织必须对各种文件进行严格的管理，结合业务和规模的变化，对文档进行有规律、周期性的回顾和修正，ISMS 要求的文件应得到保护和控制，主要控制措施有：

（1）文件发布须得到批准，以确保文件的充分性。

（2）必要时对文件进行审批与更新，并再次批准。

（3）确保文件的更改和现行修订状态得到识别。

（4）确保在使用处可获得适用文件的有关版本。

（5）确保文件保持清晰、易于识别。

（6）确保文件可以为需要者所获得，并根据适用于他们类别的程序进行转移、存储和最终的销毁。

（7）确保外来文件得到识别，并控制其分发。

（8）确保在控制状态下进行文件的发放。

（9）防止作废文件的非预期使用。

（10）若因任何原因而保留作废文件时，对这些文件进行适当的标识。

当某些文件不再适合组织的信息安全管理策略需要时，就必须将其废弃。但值得注意的是，某些文档虽然对组织来说可能已经过时，但由于法律或知识产权方面的原因，组织可以将相应文档确认后保留。

2）记录控制

在实施 ISMS 的过程中，需要对发生的各种与信息安全相关的事件进行全面的记录，从而提供符合要求和信息安全管理体系的有效运行的证据。记录应该做到以下要求：

（1）安全事件记录必须清晰，明确记录每个相关人员当时的活动。无论是书面的还是电子版的安全事件记录，都必须适当保存并进行维护，保证记录在受到破坏、损坏或丢失时容易挽救。

（2）记录应保持清晰、易于识别和检索。

（3）应编制形成文件的程序，以规定记录的储存、保护、检索、保存期限和处置所需的控制。

（4）应保留概要的过程绩效记录和所有与信息安全管理体系有关的安全事故发生的记录。

7.2.2　建立信息安全管理框架

组织建立 ISMS，首先要建立一个合理的信息安全管理框架，要从整体和全局的视角，从信息系统的所有层面进行整体信息安全建设，并从系统本身出发，通过建立资产清单，进行风险分析、需求分析和选择信息安全控制措施等步骤，建立信息安全管理体系并提出安全解决方案。

信息安全管理框架的建立必须按规范的程序进行。组织首先应根据自身的业务性

质、组织特征、资产状况和技术条件定义ISMS的总体方针和范围，然后在风险分析的基础上进行信息安全风险评估，并确定信息安全风险管理制度，选择控制目标，准备适用性声明。

1. 定义信息安全策略

信息安全策略(Information Security Policy)本质上说是描述组织具有哪些重要信息资产，并说明这些信息资产如何被保护的一个计划，其目的就是对组织中成员阐明如何使用组织中的信息系统资源，如何处理敏感信息，如何采用安全技术产品，用户在使用信息时应当承担的责任，详细描述对员工的安全意识和技能要求，列出被组织禁止的行为。

信息安全策略可以分为两个层次，一个是信息安全方针，另一个是具体的信息安全策略。

所谓信息安全方针就是组织的信息安全委员会或管理部门制定的一个高层文件，用于指导组织如何对资产，包括敏感性信息进行管理、保护和分配的规则进行指示。信息安全方针必须要在ISMS实施的前期制定出来，阐明最高管理层的承诺，提出组织管理信息安全的方法，由管理层批准，指导ISMS的所有实施工作。

除了总的信息安全方针，组织还要制定具体的信息安全策略。信息安全策略是在信息安全方针的基础上，根据风险评估的结果，为降低信息安全风险，保证控制措施的有效执行而制定的具体明确的信息安全实施规则。

信息安全策略的制定要在风险评估工作完成后，对组织的安全现状有了明确的了解的基础上有针对性地编写，用于指导风险的管理与安全控制措施的选择。

根据组织业务特征、组织结构、地理位置、资产和技术等实际情况确定ISMS方针，方针应：

(1) 包括建立目标的框架，并建立信息安全活动的总方向和总原则。

(2) 考虑业务和法律法规要求，以及合同安全义务。

(3) 根据组织战略性的风险管理框架，建立和保持ISMS。

(4) 建立风险评价的准则和定义风险评估的结构。

(5) 经过管理层的批准。

2. 定义ISMS的范围

根据组织业务特征、组织结构、地理位置、资产、技术等实际情况来确定ISMS范围。

ISMS的范围可以根据整个组织或者组织的一部分进行定义，包括相关资产、系统、应用、服务、网络和用于各种业务过程中的技术、存储以及通信的信息等，ISMS范围可以包括：

(1) 组织所有的信息系统。

(2) 组织的部分信息系统。

(3) 特定的信息系统。

3. 实施信息安全风险评估

风险评估是进行安全管理必须要做的最基本的一步，它为ISMS的控制目标与控制措

施的选择提供依据，也是对安全控制的效果进行测量评价的主要方法。

首先，组织应当确定的风险评估方法：

(1) 确定适用于ISMS、已识别的业务信息安全和法律法规要求的风险评估方法。

(2) 确定风险接受准则，识别风险的可接受等级。

(3) 风险评估方法的选择应确保可以产生可比较的、可重复的结果。

其次，组织利用已确定的风险评估方法识别风险：

(1) 识别ISMS范围内的资产及资产所有者。

(2) 识别资产的威胁。

(3) 识别可能被威胁利用的脆弱点。

(4) 识别资产保密性、完整性、可用性损失的影响。

之后，组织进行分析并评价风险：

(1) 评估安全失效可能导致的组织业务影响，考虑因资产保密性、完整性、可用性的损失而导致的后果。

(2) 根据资产的主要威胁、脆弱性、有关的影响以及已经实施的安全控制，评估安全措施失效发生的现实可能性。

(3) 估计风险的等级。

(4) 根据已建立的准则，判断风险是否可接受或需要处理。

4. 实施信息安全风险管理

该阶段主要是根据风险评估的结果进行相应的风险管理。信息安全风险管理主要包括以下几种措施：

(1) 接受风险，在确定满足组织策略和风险接受准则的前提下，有意识地、客观地接受风险。

(2) 规避风险，有些风险很容易避免，通过消除风险的原因和后果来规避风险，如在识别出风险后放弃系统某项功能或关闭系统，或通过采用不同的技术、更改操作流程、采用简单的技术措施等。

(3) 转移风险，通过使用其他措施来补偿损失，从而转移风险，将相关业务风险转嫁给他方，如保险公司、供方等。一般用于低概率、而一旦风险发生时会对组织产生重大影响的风险。

(4) 降低风险，实施适当的控制措施，把风险降低到一个可接受的级别。

5. 确定控制目标和选择控制措施

确定控制目标、选择控制措施，应考虑接受风险的准则以及法律法规和合同要求，以满足风险评估和风险处置过程所识别的要求。

从ISO/IEC 27001标准附录A中选择的控制目标和控制方式应作为这一过程的一部分，并满足这些要求。附录A的控制目标和控制方式并不详尽，可以选择其他的控制目标和控制方式。

控制目标的确定和控制措施的选择原则是成本不超过风险所造成的损失。由于信息安全是一个动态的系统工程，组织应实时对选择的控制目标和控制措施加以校验和调整，使组

织的信息资产得到有效、经济、合理的保护。

6. 准备信息安全适用性声明

适用性声明(Statement of Application,SoA)是适合组织需要的控制目标和控制措施的评论,需要提交给管理者、职员以及具有访问权限的第三方认证机构。适用性声明应包括以下两方面内容:

(1) 组织选择的控制目标和控制措施,以及选择的原因。

(2) 附录 A 中控制目标和控制措施的删减,以及删减的合理性。

适用性声明提供了一个风险处置决策的总结。通过判断删减的合理性,再次确认控制目标没有被无意识地遗漏。SoA 的准备,一方面是为了向组织内的人员声明面对信息安全风险的态度,另一方面则是为了向外界表明组织的态度和作为,表明组织已经全面、系统地审视了组织的信息安全系统,并将所有应该得到控制的风险控制在能够被接受的水平内。

7.3 信息安全管理体系的实施与运行

信息安全管理体系文件编制完成后,组织应按照文件的控制要求进行审核与批准并发布实施,至此,信息安全管理体系将进入运行阶段。体系文件通过试运行必然会出现一些问题,全体员工应将实践中出现的问题和改进意见如实反映给有关部门,以便采取纠正措施。将体系试运行中暴露出的问题,如体系设计不周、项目不全等进行协调、改进。

7.3.1 信息安全管理体系的试运行

在信息安全管理体系试运行过程中,重点注意以下问题:

1. 领导动员,以身作则

最高管理层的支持是 ISMS 有效运行的重要基础,ISMS 试运行前应该召开全体员工大会,由最高管理层作宣传动员,并承诺对组织中实施信息安全体系的支持,明确提出对各级员工信息安全职责要求,并以身作则,带头执行 ISMS 的有关规章制度。

2. 有针对性地宣传贯彻 ISMS 文件

ISMS 文件的培训工作是体系运行的首要任务,培训工作的质量直接影响体系运行的结果。组织应该按照培训工作计划的安排并按照培训程序的要求对全体员工实施各种层次的培训。培训包括信息安全意识、信息安全知识与技能和 ISMS 运行程序的培训。

3. 完善信息反馈与信息安全协调机制

体系运行过程中必然会出现一些问题,全体员工应当将实践中出现的问题,如体系设计不周、项目不全等问题进行协调、改进。信息安全管理体系的运行涉及组织体系范围的各个部门,在运行过程中,各项活动往往不可避免地发生偏离标准的现象,因此,组织应按照严

密、协调、高效、精简、统一的原则，建立信息反馈与信息安全协调机制，对异常信息加以反馈和处理，对出现的问题加以改进，完善并保证体系的持续正常运行。

4. 加强 ISMS 运行信息的管理

加强有关体系运行信息的管理，不仅是信息安全管理体系本身的需要，也是保证试运行成功的关键。所有与信息安全管理体系活动有关的人员都应按照体系文件的要求，做好信息安全的信息收集、分析、传递、反馈、处理与归档工作。

7.3.2　实施和运行 ISMS 工作

(1) 阐明风险处理计划：为管理信息安全风险，识别适当的管理措施、资源、职责和优先顺序。

(2) 实施风险处理计划：为达到已识别的控制目标，应考虑资金需求以及角色和职责分配等。

(3) 实施选择的控制措施：要实施风险分析之后选择的控制措施，以满足控制目标的需要。

(4) 评价控制措施有效性：确定如何测量所选择的控制措施或控制措施集的有效性，并指明如何用来评估控制措施的有效性，以产生可比较的和可再现的结果。

(5) 实施培训和意识教育计划：组织应通过合适的方式，如提供能力培训(必要时聘用有能力的人员)，以确保有关 ISMS 职责的人员具有相应的执行能力。

(6) 管理 ISMS 的运行。

(7) 管理 ISMS 资源。

(8) 实施能够迅速检测安全事态和响应安全事件的程序和其他控制措施。

一个可执行的风险处置计划，必然要包括以下内容：

(1) 计划的任务内容。

(2) 任务展开与执行需要的职务、权限、责任的指派。

(3) 处置计划中的技术方案与资金预算。

(4) 资源提供，包括充足数量的具备实施技术方案相应能力的人员、软件或硬件产品与工具、必要的设备等。

针对风险评估的结果，需要进行处置的风险往往不止一项，风险处置计划当然也就不止一项。对于已经识别的不可接受的风险，风险处置的目的是要将风险水平降低到可接受水平以下；出于其他业务经营的需要，组织也可能制定风险处置计划，以改变原来的可能性或后果。

针对组织的信息安全管理现状和“适用性声明”的内容，风险处置计划中的任务内容可能包括：

(1) 制定管理信息安全相关活动的规程。

(2) 对基础设施和物理安全系统进行安全加固或技术更新。

(3) 对信息系统的硬件或软件实施安全加固或技术更新。

(4) 对人员进行信息安全相关知识、技能、工具使用等项目培训、对人员进行有关风险后果的意识教育。

(5) 就信息安全管理规程的要求对人员进行培训,并推行信息安全规程。

(6) 与第三方服务提供方就信息安全管理事项进行沟通和协商,等等。

风险处置计划的实施应在受控条件下进行,做到责任分工明确。记录计划的实施,记录计划的实施结果,这些数据将可作为对信息安全管理绩效和风险处置计划实施后风险的变化进行评估的输入。

7.3.3 管理信息安全事件

信息安全事件是指系统、服务或网络的一种可识别的状态的发生,它可能是对信息安全策略的违反或防护措施的失效,或是和安全关联的一个先前未知的状态。通常情况下,信息安全事件的发生是由于自然的、人为的或者软硬件自身存在缺陷或故障造成的。

信息安全事故由单个或一系列有害或意外信息安全事件组成,它们具有损害业务运作和威胁信息安全的极大可能性。

1. 事件分类

信息安全事件的防范和处置是信息安全保障体系中的重要环节,对信息安全事件进行分级和分类是快速有效处置信息安全事件的基础之一。对信息安全事件进行合理的分级和分类将有利于促进信息的交流、共享,提高信息安全事件的通报和应急处理自动化程度、效率和效果,也有利于对信息安全事件进行统计和分析。

参考 GB/T 20986—2007《信息安全技术信息安全事件分类分级指南》可以将信息安全事件划分为有害程序事件、网络攻击事件、信息破坏事件、内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等 7 个基本分类,每个基本分类又可以分别包括若干个子类。

1) 有害程序事件

有害程序事件是指蓄意制造、传播有害程序,或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序,有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性,或影响信息系统的正常运行。有害程序事件包含 7 个子类事件:计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件、其他有害程序事件。

2) 网络攻击事件

网络攻击事件是指通过网络或其他技术手段,利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力对信息系统实施攻击,并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包含 7 个子类事件:拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件、其他网络攻击事件。

3) 信息破坏事件

信息破坏事件是指通过网络或其他技术手段,造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包含 6 个子类事件:信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件、其他信息破坏事件。

4) 信息内容安全事件

信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利

益的内容的安全事件。信息内容安全事件包含4个子类事件：违反宪法和法律、行政法规的信息安全事件；针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件；其他信息内容安全事件。

5）设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为地使用非技术手段有意或无意地造成信息系统破坏而导致的信息安全事件。设备设施故障事件包括4个子类事件：软硬件自身故障、外围保障设施故障、人为破坏事故、其他设备设施故障。

6）灾害性事件

灾害性事件是指由于不可抵抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

7）其他信息安全事件

其他信息安全事件类别是指不能归为以上6个基本分类的信息安全事件。

2．事件分级

对信息安全事件进行分级主要考虑信息系统的重要程度、系统损失和对社会造成的影响等三个基本要素。

信息系统的重要程度主要考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性，以及业务对信息系统的依赖程度，划分为特别重要信息系统、重要信息系统和一般信息系统。

系统损失是指由于信息安全事件对信息系统的软硬件、功能及数据的破坏，导致组织业务中断，从而给事发组织和国家所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价。

社会影响是指信息安全事件对社会所造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响。

通常把事件划分为特别重大、重大、较大和一般4个级别。

1）特别重大事件

特别重大事件是指能够导致严重影响或破坏的信息安全事件，它造成的影响或破坏有：会使特别重要信息系统遭受特别严重的系统损失；产生特别重大的社会影响。

2）重大事件

重大事件是指能够导致严重影响或破坏的信息安全事件，它造成的影响或破坏有：会使特别重要信息系统遭受严重的系统损失，或使重要信息系统遭受特别严重的系统损失；产生重大的社会影响。

3）较大事件

较大事件是指能够导致较严重影响或破坏的信息安全事件，它造成的影响或破坏有：会使特别重要信息系统遭受较大的系统损失，或使重要信息系统遭受严重的系统损失，一般信息系统遭受特别严重的系统损失；产生较大的社会影响。

4）一般事件

一般事件是指不满足以上条件的信息安全事件，它造成的影响或破坏有：会使特别重要信息系统遭受较小的系统损失或使重要信息系统遭受较大的系统损失、一般信息系统遭受严重或严重以下级别的系统损失；产生一般的社会影响。

3. 应急组织机构

1）国内外知名应急组织机构

国内外比较知名的应急组织机构有如下三个：

1988 年的"莫里斯蠕虫事件"造成占当时全部联网计算机中 10%陷入瘫痪，世界上第一个应急响应组织源自于此。事件发生后，美国国防部高级计划研究署(Defense Advanced Research Projects Agency，DARPA)出资在卡耐基·梅隆大学(Carnegie Mellon University，CMU)的软件工程研究所(Software Engineering Institute，SEI)建立了计算机应急处理协调中心(Computer Emergency Response Team/Coordination Center，CERT/CC)。

随着信息技术的不断发展，中国教育和科研计算机网(China Education and Research Network，CERNET)于 1999 年建成国内第一个网络紧急响应中心，即中国教育和科研网紧急响应组(CERNETCERT，CCERT)，专注于计算机网络安全事件的应急处理。除了网络安全应急组之外，中国教育与科研网针对计算机安全事件还组建了物理环境、网络信息和网络运行等多个应急处置组，这些应急处置组与网络安全应急组在应急处置管理小组的统一指挥协调下，从不同方面和层次共同应对计算机安全事件。

国家计算机网络应急处理协调中心(National Computer Network Emergency Response Technical Team/Coordination Center of China，CNCERT/CC)是在国家因特网应急小组协调办公室的直接领导下，协调全国范围内计算机安全应急响应小组(CSIRT)的工作以及与国际计算机安全组织的交流。CNCERT/CC 还负责为国家重要部门和国家计算机网络应急处理体系的成员提供计算机网络应急处理服务和技术支持。

2）单位应急响应工作机构

对于一个单位来说，可以建立自己的应急响应工作机构，包括应急领导小组、应急工作小组和应急响应小组，主要组成及职责如下：

(1) 应急领导小组

负责本单位应急响应工作的统筹规划和决策指挥。应急领导小组成员由本单位行政主管及业务部门、技术部门、后勤部门等部门负责人组成。一般应由本单位的行政主管担任小组领导。应急领导小组负责统筹规划本单位的应急响应工作，确定本单位应急响应工作的基本内容和重点，组建应急工作小组和应急响应小组；负责对本单位应急响应工作重要事项做出决策，包括批准本单位应急预案发布施行、确定重大信息安全事件响应方案等；统一指挥本单位应急响应的各项工作，包括日常应急准备工作和发生信息安全事件时的应急响应工作。

(2) 应急工作小组

负责本单位各项应急准备工作。应急工作小组由本单位的应急领导小组负责组建，并接受该小组的统一指挥。应急工作小组可不单独设立，但必须明确组成人员的职责分工。应急工作小组的工作主要包括制定应急预案、准备应急资源、进行应急响应培训和应急演

练等。

（3）应急响应小组

负责发生信息安全事件时的应急响应工作。应急响应小组由本单位的应急领导小组负责组建，并接受该小组的统一指挥。应急响应小组可以不单独设立，但必须明确组成人员的职责分工，保证本单位的各项应急响应工作都有确定的人员负责完成。发生信息安全事件时，应急响应小组立即转换为实体形式并投入应急响应工作。应急响应小组的工作主要包括对突发信息安全事件进行分类、分级，并及时上报，组织开展应急响应工作。

4. 应急处置流程

突发信息安全事件的应急处置过程主要包括事件上报和接报、处置、报告、总结等。

1）事件上报和接报

单位内部工作人员、协作单位或者第三方人员发现安全事件或者安全漏洞后应立即报告应急响应小组。事件报告的内容包括报告人、单位名称、联系方式、事件范围、事件类别、事件后果、影响范围、事件基本现象的描述、用户判断的事件原因等。

2）事件处置

应急响应小组到达事发现场后，应立即开展现场保护工作，防止证据、关键信息的丢失，应急响应工作人员根据现场实际情况决定是否进行调查取证、攻击追踪、抑制工作，随后应立即展开现场数据收集、分析、确认、清理、恢复等工作。当需要上层决策支持时，应急响应小组应及时上报应急工作小组，由应急工作小组或应急领导小组决策采取进一步的措施。

3）事件报告

应急响应小组完成现场处置后，应及时将事件处置结果、原因分析等形成正式报告上报应急工作小组。

4）事件总结

应急工作小组、应急响应小组对每次事件的事发原因、处理过程、事件原因、造成损失等进行总结，研究针对类似事件的预防、解决措施，防止类似事件的再次发生。

7.3.4 保持 ISMS 持续有效

体系通过试运行的完善，体系的充分性与适宜性得到了保证，下一步工作的重点就是进入正式运行阶段，并保持信息安全体系的持续有效。组织可以通过定期的体系审核来验证体系的有效性，并对发现的问题采取有效的纠正措施并实施，对纠正措施实施的结果进行验证；信息安全管理体系的运行环境不可能永远保持不变，当组织的信息系统、组织结构等情况发生重大变更时，组织应根据风险评估的结果对体系进行适当的调整。

ISMS 毕竟仅仅提供一些原则性的建议，如何将这些原则性的建议与各个组织单位自身的实际情况相结合，构架起符合组织自身状况的 ISMS，并使有效运行，才是真正具有挑战性的工作。在建立和运行安全的信息系统时，信息安全技术、信息安全产品是信息安全管理的基础，信息安全管理是信息安全的关键，人员管理是信息安全管理的核心，信息安全策略是进行信息安全管理的指导原则，信息安全管理体系规范建立与有效运行是实现信息安全管理最为有效的手段。

7.4 信息安全管理体系的审核

7.4.1 审核的概念

1. 审核概念

体系审核是组织为获得审核证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程。

ISMS 审核是 ISMS 审核人员为了获得审核证据，而独立地、客观地、正式地和有计划地评估被评审组织的 ISMS，确定其对 ISMS“审核准则”符合程度所进行的一系列活动。审核的结果产生一个书面的“审核报告”。

ISMS 审核包括管理和技术两方面的审核，管理性审核主要是定期检查有关信息安全方针、策略与规程是否被正确有效地实施；技术性审核是指定期检查组织的信息系统符合信息安全实施标准的情况，技术性的审核需要信息安全技术人员的支持，必要时会使用系统审核工具。

2. 审核目的

组织应建立并保持审核方案和规程，定期开展信息安全管理体系的审核，以保证它的文件化过程，信息安全活动以及实施记录能够满足 ISO/IEC 27001 的标准要求和声明的范围，检查信息安全实施过程符合组织的方针、目标和策划要求，并向管理者提供审核结果，为管理者的信息安全决策提供支持。

ISMS 审核的主要目的如下：

(1) 检查 ISO/IEC 27001 的实施程度与标准的符合性情况。

(2) 检查满足组织安全策略与安全目标的有效性和适用性。

(3) 识别安全漏洞与弱点。

(4) 给管理者提供 IT 安全控制目标实现状况，使管理者了解 IT 安全问题。

(5) 指出存在的重大的控制弱点，证实存在的风险。

(6) 建议管理者采用正确的校正行动，为管理者的决策提供有效支持。

(7) 满足法律、法规与合同的需要。

(8) 提供改善 ISMS 的机会。

3. 审核分类

ISMS 审核可分为两种，一是内部信息安全管理体系审核，也称第一方审核，是组织的自我审核；二是外部信息安全管理体系审核，也称第二方、第三方审核。第二方审核是顾客对组织的审核，第三方审核是第三方性质的认证机构对申请认证组织的审核。这两种审核在审核的目的、审核方组成、审核依据、审核人员及审核后的处理等方面均不同。表 7-2 列出了它们的区别。

表 7-2　内、外部 ISMS 体系审核比较表

	内部 ISMS 审核	外部 ISMS 审核
目的	审核 ISMS 的符合性、有效性，采取纠正措施，使体系正常运行和持续改进	第二方：选择合适的合作伙伴；证实合作方持续满足规定要求；促进合作方改进信息安全管理体系 第三方：导致认证、注册
审核方	第一方	第二方、第三方
依据	ISO/IEC 27001 标准 ISMS 文件 适用于组织的有关 ISMS 法规及其他要求	第二方：合同，企业 ISMS 文件；适用于被审核方的 ISMS 法规及其他要求 第三方：ISO/IEC 27001 标准；企业 ISMS 文件；适用于被审核方的 ISMS 法规及其他要求
审核方案	集中式/滚动式审核	集中式审核
审核员	有资格的内审员，也可聘外部审核员	第二方：自己或外聘审核员 第三方：注册审核员
文件审查	根据需要安排	必须进行
审核报告	提交不符合报告和采取纠正措施的建议	只提交不符合报告
纠正措施	重视纠正措施。对纠正措施计划可提方向性意见供参考，对纠正措施完成情况不仅要跟踪验证，还要分析研究其有效性	对纠正不能作咨询，对纠正措施计划的实施要跟踪验证
监督检查	无此内容	认证或认可后，每年至少进行一次监督检查

4. 审核步骤

ISMS 审核的主要步骤如下：

（1）审核计划。

（2）审核准备。

（3）现场审核。

（4）编写审核报告。

（5）纠正措施的跟踪。

（6）全面审核报告的编写和纠正措施计划完成情况的汇总分析。

7.4.2　ISMS 内部审核

1. 内部审核基本内容

组织应按策划的时间间隔进行 ISMS 内部审核，以确定组织 ISMS 的控制目标、控制措施、过程和程序是否达到下述要求：

（1）符合标准及相关法律法规的要求。

（2）符合已识别的信息安全要求。

（3）得到有效的实施和保持。

(4) 按期望运行。

应策划审核方案，考虑被审核区域的审核过程和区域的状况及重要性，以及审核的结果。应规定审核准则、范围、频次和方法。审核员的选择和审核的实施应保证审核过程的客观和公正。审核员不能审核自己的工作。

应建立形成文件的程序，以规定策划和实施审核、报告结果和保持记录的职责和要求。

被审核区域的负责人应确保立即采取措施以消除发现的不符合及其原因。跟踪活动应包括所采取措施的验证以及验证结果的报告。

2. 内部审核流程

1) 内部审核策划

内部审核周期及范围：正常情况下，公司信息安全管理体系内部审核至少每年组织一次，两次时间间隔不得超过 12 个月。出现下列情况时可由管理者决定是否增加信息安全管理体系的内部审核次数：

(1) 组织结构和职能分工出现重大变化。

(2) 业务内容出现重大变化。

(3) 信息安全管理体系出现重大变化。

(4) 采用标准、适用法律或验证方法出现重大变化。

(5) 出现重大客户投诉或信息安全事故。

(6) 其他需要增加内审的情形。

信息安全管理体系审核对象为公司信息安全管理体系所涉及的部门和活动。审核范围可以是对公司进行整体审核，也可以按部门或过程进行局部审核。正常情况下，管理体系所涉及的所有部门和过程每年至少应覆盖一次。其中各部门或各过程的审核频次还应取决于其现状和重要程度，并考虑以往审核的结果。计划外的追加审核由管理者根据实际情况确定。

2) 内部审核组织

(1) 由管理者负责组织内审小组，并填写《内审组长成员任命书》。

(2) 内部审核员通常要求由接受过信息安全管理体系内部审核培训并取得资格证书的人员组成，审核员应与被审核的活动无直接责任，审核员不应审核自己的工作，以保证审核的独立性，内部审核员应在公司内各部门挑选并经公司任命。

(3) 内审组长应由管理者从内审员中指定，管理者可以自己担任审核组长。

3) 内部审核计划

(1) 内审组长负责组织制定和提出《内部审核计划》。

(2)《内部审核计划》应包含审核目的、审核范围、审核时间和进度安排、审核成员、审核的注意事宜等；审核时间的安排需要和被审核部门事先协调。

(3)《内部审核计划》由管理者审批后实施；管理者自己担任内审组长的情况下，需要组织内审小组其他成员对计划进行审核。

4) 内部审核准备

(1) 各审核员应准备好并熟悉本次审核所依据的文件：如标准、信息安全管理手册、有关程序文件、合同、法律法规、客户及相关方要求等。

（2）内审小组成员根据分工，编制《内审检查表》，并报内审组长批准。

5）内部审核实施

内部审核实施可划分为首次会议、现场审核和末次会议三个阶段进行。

由内审组长召开首次会议，参加的人员由内审员及被审核部门负责人组成。在会议上，内审组长将介绍：

（1）内审小组成员、审核目的、范围。

（2）审核方法、依据和程序。

（3）提出审核要求，确认审核日程安排等。

（4）公布末次会议日期、时间、会议内容及参加人员。

（5）审核计划中需说明的其他细节问题。

现场审核包括下述内容：

（1）现场审核时，内审员根据《内审检查表》逐项进行审核，通过观察、提问、查阅文件和记录、抽样、问题追踪等方法，以验证审核情况与体系的符合性。

（2）内审员应如实记录审核的情况，对发现的不符合项应详细记录并由被审核部门负责人或直接责任人确认，以保证不符合项已经得到被审核部门的理解，便于纠正和预防。

（3）现场审核结束后，内审组长召开内部内审小组成员会议，听取内审员的审核情况汇报、复核发现的不符合项、编写《不符合项报告及纠正报告单》。

（4）内审组长应与受审核部门领导进行沟通，提出《不符合项报告及纠正报告单》，由被审核部门签字确认，并责成相关部门按要求制定纠正及预防措施，并填写在《不符合项报告及纠正报告单》上。

末次会议包括以下内容：

（1）末次会议由内审组长主持，由内审小组成员、受审核方负责人、不符合项相关人员参加。

（2）由内审小组通报审核结果，内容可包括：报告审核情况；通报不符合项及其严重程度；提出制定纠正措施、改进对策的限期；本次审核结论。

6）公司内审报告

完成信息安全管理体系内审后，由内审组长起草编写审核报告，审核报告内容需包括：

（1）审核目的、审核范围、审核依据和审核时间。

（2）内部审核组成员及其分工。

（3）被审核的部门。

（4）内部审核情况综述。

（5）不符合项的综合分析。

（6）对被审部门的评价、审核结论。

（7）存在问题的分析及管理体系改进措施的建议。

《公司内审报告》经管理者批准后，以打印或以电子文档的方式分发给被审核部门。《公司内审报告》由内审小组负责整理归档。

7）纠正不符合项

《不符合项报告及纠正报告单》由内审小组统计后分发到各责任部门，由责任部门分析不符合原因，制定纠正措施，经内审组长确认后，由责任部门组织实施。

8）跟踪和验证

（1）审核小组在限定时间内对纠正措施的实施情况进行复审，以确认不符合项的纠正情况并验证其有效性。

（2）责任部门已完成纠正措施后，通知内审员验证其完成情况和有效性，并由内审员在《不符合项报告及纠正报告单》上签名认可。

（3）不符合项复审仍不符合的项目，其部门负责人应说明原因并考虑是否需要重新制定纠正预防措施。

（4）如在规定的日期内不能完成的，内审员应检查不能完成的原因，无正当理由的应报管理者批准后，重新开出《不符合项报告及纠正报告单》并且必须在规定的日期内关闭。

（5）内部审核实施和验证情况由内审组长向管理者报告。

（6）审核记录归档。

本程序所涉及的所有记录(内部审核计划、内审检查表、内审报告等)由内审小组按《记录控制程序》统一归档保存。

3. 实施策略

（1）管理者负责成立内审小组，并任命内审组长，发布《内审组长成员任命书》。

（2）内审组长负责组织编写并审核批准《内部审核计划》。

（3）各内审员根据分工编写《内审检查表》。

（4）由内审组长召开首次会议，并填写首次会议的《会议签到记录表》。

（5）各内审员根据计划进行内审，发现不符合项，填写《不符合项报告及纠正报告单》，跟踪不符合项的解决。

（6）由内审组长召开末次会议，并填写末次会议的《会议签到记录表》。

（7）内审结束后，内审组长负责编写《公司内审报告》。

7.4.3 信息安全管理体系管理评审

1. 管理评审的定义

管理评审主要是指组织的最高管理者按规定的时间间隔对信息安全管理体系进行评审，以确保体系的持续适宜性、充分性和有效性。管理评审过程应确保收集到必要的信息，以供管理者进行评价，管理评审应形成文件。

管理评审应根据信息安全管理体系审核的结果、环境的变化和对持续改进的承诺，指出可能需要修改的信息安全管理体系方针、策略、目标和其他要素。

管理评审总目标是检查信息安全管理体系的有效性，至少每年一次，以识别需要的改进和采取的行动。在确定目前的安全状态是否令人满意的同时，应注意技术的变化和业务需求的变化及新威胁和脆弱点的发生，以预测信息安全管理体系未来的变化，并确保其在未来持续有效。

管理层应按策划的时间间隔评审组织的信息安全管理体系，以确保其持续的适宜性、充分性和有效性。评审应包括评价信息安全管理体系改进的机会和变更的需要，包括安全方针和安全目标。评审的结果应清楚地文件化，应保持管理评审的记录。

2. 职责与权限

（1）公司高管：主持召开管理评审大会，批准《管理评审报告》。

（2）管理者：批准《管理评审计划》，组织召开管理评审会，组织撰写《管理评审报告》。

（3）主管体系建设部门：制定《管理评审计划》，负责搜集并提供管理评审资料，负责对评审后的纠正、对预防措施进行跟踪和验证。

（4）各部门：准备、提供与本部门工作相关的评审所需的资料，负责实施管理评审中提出的相关的纠正及预防措施。

3. 评审输入

管理评审的输入应包括以下几个方面的信息：

（1）信息安全管理体系审核和评审的结果。

（2）相关方的反馈。

（3）可以用于组织改进其信息安全管理体系绩效和有效性的技术、产品或程序。

（4）预防和纠正措施的状况。

（5）以往风险评估没有足够强调的脆弱性或威胁。

（6）以往管理评审的跟踪措施。

（7）任何可能影响信息安全管理体系的变更。

（8）改进的建议。

4. 评审输出

管理评审的输出应包括以下几个方面有关的任何决定和措施：

（1）对信息安全管理体系有效性的改进。

（2）风险评估和风险处置计划的更新。

（3）修改影响信息安全的程序，必要时，回应内部或外部可能影响信息安全管理体系的事件，包括以下的变更：业务要求；安全要求；业务过程影响现存业务的要求；法规或法律环境；合同义务；风险的等级和/或可接受风险的水平。

（4）资源需求。

（5）如何测量控制措施有效性的改进。

5. 制定年度管理评审计划

组织主管部门根据信息安全管理体系的运营情况，根据《信息安全管理手册》以及 ISO/IEC 27001 的标准要求，于每年年初制定《年度管理评审计划》。管理评审计划由管理者审批后方可生效。

管理评审计划的主要内容包括：审核目的、审核范围、审核准则、审核组的组建、审核员的资质、审核的时间、参与评审的部门等要求。

管理评审一般每年进行一次，一般在同一年度最后一次内部审核完成后进行，也可根据需要安排。当出现下列情况之一时可适当增加管理评审频次：

（1）公司组织机构、服务范围、资源配置发生重大变化。

(2) 发生重大 IT 服务事故/安全事故或用户关于 IT 服务/信息安全有严重投诉或投诉连续发生。

(3) 法律、法规、标准及其他要求有变化。

(4) 市场需求发生重大变化。

(5) 即将进行第二、三方审核。

(6) 审核中发现严重不符合。

管理评审实施计划由主管体系建设部门组织制定。主管体系建设的部门于每次管理评审前一个月编制《管理评审计划》,报管理者审批。计划主要内容包括:评审时间;评审目的;评审依据;评审内容;评审范围及评审重点;参加评审部门及人员;各部门应该准备的资料以及提交时间。

6. 资料准备

预定评审前一周,主管体系建设的部门组织、指导、督促各部门完成本部门应该提交的资料,以书面形式向管理者汇报。管理者认为资料准备不全、信息不够充分的,主管体系建设的部门组织相关责任部门按照管理者的要求进一步补充完善。

7. 管理评审会议

管理评审会议召开前 2～7 天,会议组织者应向与会人员以书面或邮件形式发送《管理评审会议通知》,并整理与会人员的反馈,以确定与会人员的实际人数。

管理者主持管理评审会议,各部门负责人和有关人员对评审输入做出评价,对于发现的不符合项或潜在的不符合项提出纠正和预防措施,确定责任人和整改时间。

管理者对所涉及的评审内容做出结论,包括进一步调查、验证等。

管理评审采取什么方式进行由管理者请示公司领导后决定,一般默认情况下以会议形式进行。

管理评审会议应指定专人做会议记录。

8. 管理评审报告

管理评审大会结束后,由体系主管部门根据管理评审输出的要求和管理评审大会的会议记录进行总结,在管理者的指导下撰写《管理评审报告》,经管理者审核,交领导批准后,发至相关部门并由主管体系建设的部门负责监控执行。

如果评审结果引起文件更改,应执行《文件控制程序》。

管理评审产生的相关的记录应由主管体系建设的部门按《记录控制程序》保管,包括管理评审计划、评审前各部门准备的评审资料、评审会议记录及管理评审报告等。

9. 相关支持性文件和记录

《文件控制程序》

《记录控制程序》

《内部审核程序》

《管理评审计划》

《管理评审会议通知》
《管理评审报告》
《管理评审会议记录》
《年度管理评审计划》

10. 管理评审的后续工作

管理评审的结果应予以记录并保存，如管理评审计划、各种输入报告、管理评审报告、纠正措施及其验证报告等。

信息安全管理部门的负责人员还要组织有关部门对管理评审中的纠正措施进行跟踪验证，验证的结果应记录并上报最高管理层及有关人员。

7.5　信息安全管理体系的改进与保持

7.5.1　持续改进

组织应通过应用信息安全策略、安全目标、审核结果、监视事件的分析、纠正预防措施和管理评审，持续改进 ISMS 的有效性。

组织应定期进行：

（1）实施 ISMS 已识别的改进。

（2）采取适当的纠正和预防措施，总结从其他组织或组织自身的信息安全经验得到的教训。

（3）与所有相关方沟通措施和改进，沟通的详细程度应与环境相适宜，必要时应约定如何进行。

（4）确保改进活动达到了预期的目的。

7.5.2　纠正措施

组织应采取措施，消除与 ISMS 要求不符合的原因，以防止再发生。纠正措施文件程序应规定以下方面的要求：

（1）识别不符合。

（2）确定不符合的原因。

（3）评价确保不符合不再发生所需的措施。

（4）确定和实施所需的纠正措施。

（5）记录所采取措施的结果。

（6）评审所采取的纠正措施。

7.5.3　预防措施

组织应采取措施，以消除与 ISMS 要求潜在不符合的原因，以防止发生，所采取的预防措施应与潜在问题的影响相适宜。预防措施文件程序应规定以下方面的要求：

(1) 识别潜在不符合及其原因。

(2) 评价预防不符合发生所需的措施。

(3) 确定并实施所需的预防措施。

(4) 记录所采取措施的结果。

(5) 评审所采取的预防措施。

预防不符合的措施通常比纠正措施更有效。组织应识别发生变化的风险,并通过关注变化显著的风险来识别预防措施要求,应根据风险评估结果来确定预防措施的优先级。

思考题

1. 组织内部成功实施信息安全管理体系的关键因素包括哪些内容?
2. 信息安全管理体系中管理承诺包括哪些内容?
3. 试述信息安全管理体系总体工作计划的主要内容。
4. 信息安全管理体系文件包括哪些内容?
5. 试述信息安全管理体系文件的作用和文件的层次。
6. ISMS 审核有哪几种分类?说明类别之间的联系与区别。
7. 试述信息安全管理体系内部审核流程的主要内容。
8. 试归纳信息安全管理体系管理评审流程。

第8章 信息安全管理体系的认证

8.1 信息安全管理认证

8.1.1 认证的定义

认证是第三方依据程序对产品、过程、服务符合规定的要求给予书面保证(合格证书),认证的基础是标准,认证的方法包括对产品特性的抽样检验和对组织体系的审核与评定,认证的证明方式是认证证书与认证标志。认证是第三方所从事的活动,通过认证活动,组织可以对外提供某种信任与保证,如产品质量保证、信息安全保证等。

信息安全认证包括两类:一类为 ISMS 认证,另一类为信息安全产品认证。

组织实施信息安全管理体系认证,就是根据 ISO/IEC 27001 标准,建立完整的信息安全管理体系,达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式,用最低的成本,达到可接受的信息安全水平,从根本上保证业务的持续性。

8.1.2 认证的目的和作用

信息安全管理第三方认证为组织的信息安全体系提供客观公正的评价,使组织在信息安全管理方面有更大的可信性,并且能够使用证书向利益相关的组织提供保证;同时,认证能够促进组织间的贸易关系,提高跨行业的信息安全管理水平,从整体上有利于全球贸易的开展。

信息安全管理体系可以保证组织提供可靠的信息安全服务,对该体系进行认证可以树立组织信息安全形象,为客户、合作者提供信息安全信任感,有利于组织业务活动的开展,特别是当信息安全构成组织所提供产品或服务的一个质量特性时,如金融、电信等服务组织,开展 ISO/IEC 27001 体系认证对外具有很强的质量保证作用。

ISMS 第三方认证为组织的信息安全管理体系提供客观公正的评价,使组织在信息安全管理方面具有更大的可信性,并且能够使用证书向利益相关的组织提供保证。信息安全管理体系认证的目的和作用一般包括以下几个方面:

(1) 获得最佳的信息安全运行方式。

(2) 保证业务安全。

(3) 降低风险、避免损失。

(4) 保护核心竞争优势。

（5）提高商业活动中的信誉。
（6）增加竞争能力。
（7）满足客户要求。
（8）保证可持续发展。
（9）符合法律法规要求。

8.1.3 认证范围

在向认证机构表达认证范围时要注意，组织寻求的认证范围应该与信息安全管理体系建立的范围是相同的。例如，组织可能有几个办公地点，安全管理系统在这几个地点进行，但是可能只需申请对一个办公地点的认证。

认证范围定义是审核员确定评估计划的基础。认证机构将选择需要评估的功能和活动，并评估审核的时间，以及选择有适当背景的审核员与技术专家。

认证范围声明应该表达清楚，易于阅读，并吸引潜在的贸易伙伴的注意。在拟定认证范围时，需要考虑下列因素：

（1）文件化的适用性声明。
（2）组织的相关活动。
（3）要包含在内的组织的范围。
（4）地理位置。
（5）信息系统边界、平台。
（6）所包含的支持活动。
（7）例外情况。
（8）在开展认证过程之前认证机构需要对认证范围进行认可。

8.2 认证的基本条件与认证机构的选择

8.2.1 认证条件

组织按照 ISO/IEC 27001 标准与适用的法律法规要求，建立并实施文件化的信息安全管理体系，并满足以下基本条件以后，可以向被认可的认证机构提出认证申请：

（1）遵循法律、法规的努力已被相关机构认同。
（2）信息安全管理体系文件完全符合标准要求。
（3）信息安全管理体系已被有效实施，即组织在风险评估的基础上识别出需要保护的关键信息资产、制定信息安全方针、确定安全控制目标与控制方式并实施、完成体系审核与评审活动并采取相应的纠正预防措施。

8.2.2 认证机构

组织在具备体系认证的基本条件时，就可以寻求认证机构申请体系认证。

中国信息安全认证中心是经中央编制委员会批准成立，由国务院信息化工作办公室、国

家认证认可监督管理委员会等八部委授权，依据国家有关强制性产品认证、信息安全管理的法律法规，负责实施信息安全认证的专门机构。中国信息安全认证中心为国家质检总局直属事业单位，基于国际标准 ISO/IEC 27001：2005 实施信息安全管理体系认证。

组织在选定认证机构后，就可以与之联系提交认证申请，在双方协商一致的情况下签订认证合同，认证费用是按照审核员的审核人天数(包括文件审核与完成审核报告的人天)与每人天的审核价格来计算。认证合同中应明确认证机构保守组织商业秘密，在组织现场遵守组织的有关信息安全规章的要求。审核所需的人天数取决于以下因素：

(1) 被审核组织认证范围的员工数。

(2) 认证范围持有的信息量。

(3) 场所数据与地理位置分布。

(4) 与外界的接触面。

(5) 所利用的信息技术的复杂程度。

(6) 组织是否已具有一个相关的管理体系认证证书。

(7) 业务功能。

(8) 企业类型。

(9) 风险程度。

8.3　信息安全管理体系的认证过程

信息安全管理体系认证的总体流程如图 8-1 所示。

8.3.1　认证的准备

在认证之前，认证方与被认证方都要进行相应的准备活动。

被认证方需要按照 ISO/IEC 27001 建立信息安全管理体系，在确认满足认证基本条件的情况下，被认证方向认证机构递交正式申请；认证机构对被认证方的申请资料进行初步检查，确定是否受理申请。如受理申请，认证机构将评估认证费用和正式审核时间。

组织可以寻求认证的类型，如整个组织，包括所有的信息设施、特定的信息系统。

组织为认证要做的准备工作，包括文件化的信息安全方针、策略、程序、适用性声明及其他文件。

确定 ISMS 范围，以及此范围内的组织结构、人员组成、业务场所的数目、功能、信息安全的应用、业务特性、风险程序等相关材料；已建立适当的安全组织和必要的基础设施，与信息安全相关的员工已落实明确的安全责任的相关说明资料；ISMS 范围业务体系的描述，与外界的接口；法律、法规、合同的附加要求；采用了有效的风险评估和风险管理方法，对认证范围所有信息系统进行了风险评估，根据 ISO/IEC 27001 的标准要求，建立有效文件，将所有类型的安全风险和 ISO/IEC 27001 控制联系起来，并成功地选择了安全控制目标与控制措施；组织有适当的风险接受的处理程序；文件化的信息安全检查列表，可以证明安全控制正在被正确地实施，并经过相关测试；文件化的安全维护和管理的过程；文件化的体系审核和管理评审报告。

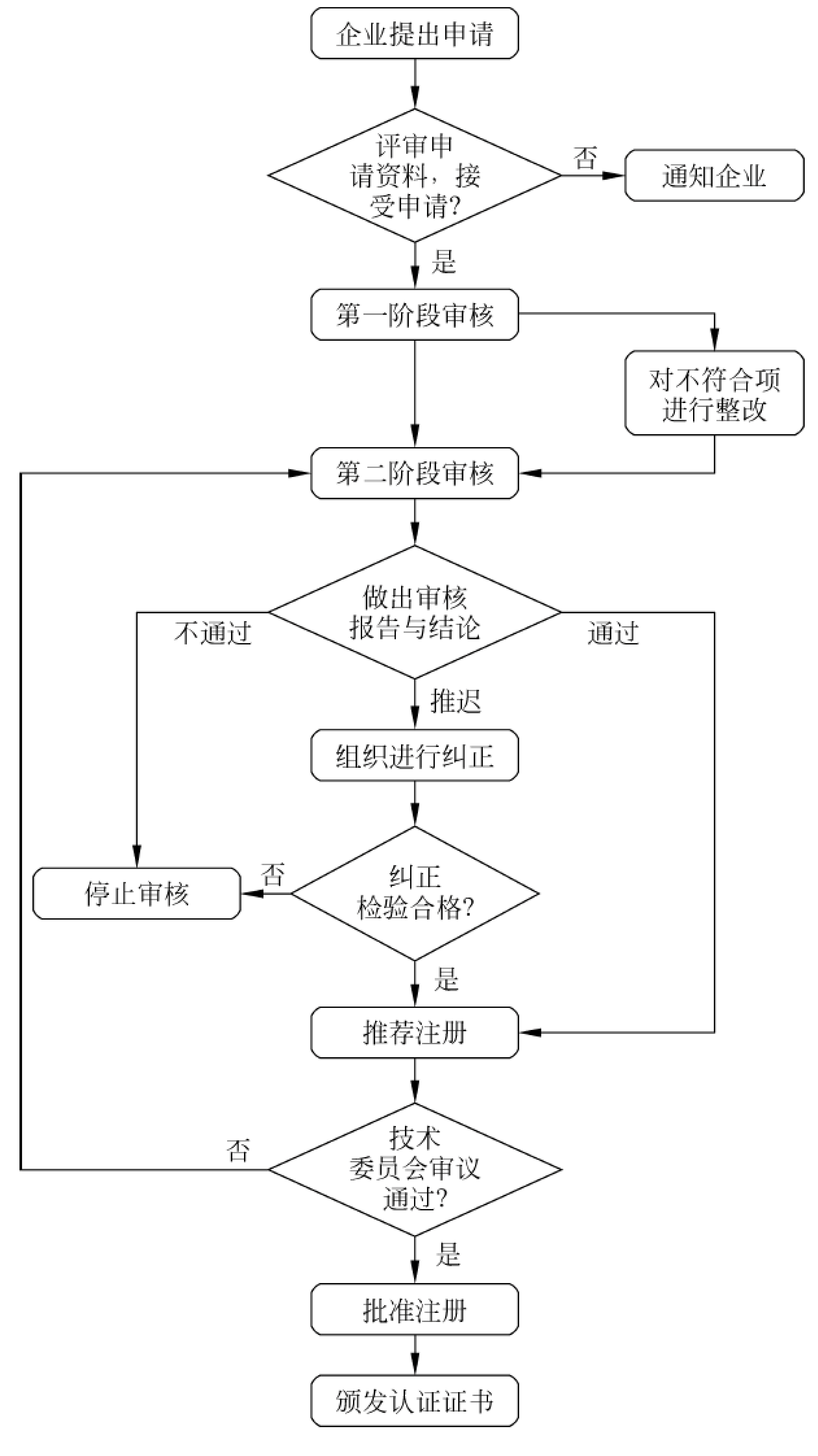


图 8-1　ISMS 认证的过程

8.3.2　认证的实施

1. 文件审核与初访

第一阶段主要是从总体上了解被审核方 ISMS 的基本情况，确认被审核方是否具备认证审核条件，为第二阶段的审核策划提供依据。审核的重点在于审核 ISMS 文件是否符合 ISO/IEC 27001 标准的要求，了解被审核方的活动、产品或服务的全过程，判断风险评估与风险管理状况，并对被审核方 ISMS 的策划及内审情况等进行初步审查。

(1) 文件审核。通常文件审核包括以下内容：

① 认证范围、适用性声明。

② 信息安全方针、策略、程序、作业指导书。

③ 信息系统环境文件(信息基础设施、网络拓扑结构、信息系统相关人员)。

④ 风险评估与风险管理文件。

⑤ 业务持续性计划。

⑥ 体系审核和管理评审报告。

⑦ 法律、法规、合同的要求。

⑧ 信息安全记录。

(2) 第一阶段现场审核准备,包括以下内容:

① 确定现场审核日期。

② 编制第一阶段现场审核计划。

③ 编制检查表。

(3) 第一阶段现场审核,包括以下内容:

① 见面会。审核组与被审核组织的管理者、信息安全管理经理及有关人员会面,说明第一阶段审核的目的、范围、内容、程序和方法,识别评审难点,并陈述保密声明。

② 现场检查。

③ 与信息安全管理经理交谈,了解被审核组织基本情况以及信息安全管理体系整体运行情况。

④ 到现场调查,了解信息资产、威胁、脆弱点识别是否有遗漏,风险评估与风险管理程序是否适宜,主要方式是审核文件、查阅记录。

⑤ 检查组织的法律、法规获取识别情况以及法律、法规符合性。

⑥ 检查并评审组织的内审情况。

⑦ 检查并评审组织的 ISMS 策划的可行性和适用性。包括 ISMS 方针、策略、程序、控制目标、控制措施、运行策划等。

⑧ 证实管理评审已实施。

⑨ 开不符合项报告。

⑩ 交流会。现场审核结束前,召开交流会,审核组长向被审组织通报第一阶段审核结论,指出存在的不符合项,提出纠正要求,并确定第二阶段审核的条件和具体事宜。

(4) 第一阶段审核报告,报告的编制包括以下内容:审核的实施情况与审核结论、发现的问题及下一步的工作重点。

第一阶段与第二阶段审核的差异如表 8-1 所示。

2. 全面审核与评价

第二阶段审核是对信息安全管理体系的全面审核与评价,目的是验证组织的信息安全管理体系是否按照认证标准与组织体系文件要求予以有效实施,组织的安全风险是否被控制在组织可以接受的水平内,根据审核发现对组织的信息安全管理体系运行状况是否符合标准与文件规定做出判断,并据此对被审核方能否通过信息安全管理体系认证做出结论。

1) 第二阶段的审核准备

审核组综合考虑第一阶段审核结论及被审核方对不符合项的纠正情况,确定进行第二阶段审核的时机和条件是否成熟。在此基础上,审核组进行第二阶段审核的准备工作:确定现场审核日期、编制第二阶段现场审核计划、编制检查表。

表 8-1 第一阶段与第二阶段审核的差异

	第 一 阶 段	第 二 阶 段
目的	• 了解 ISMS 状况,确认被审核方是否具备认证审核条件; • 确定第二阶段审核的可行性; • 确定第二阶段审核的重点	• 评价被审核方的 ISMS 是否有效实施; • 决定被审核方能否通过认证审核并取得注册
范围	• 被审核方的 ISMS 文件和有关资料; • 与重要信息资产极高风险源有关的现场	• 所有现场和有关文件与资料
审核人日	• 较少(约占总人日的 1/3～1/4)	• 较多(约占总人日的 2/3～3/4)
审核内容	• 适用的法律、法规的识别与满足的基本情况; • 风险评估、风险管理方法策划的充分性; • 方针、策略、控制目标、控制措施的连贯性、适宜性; • 对实现信息安全方针与目标的策划; • 组织内容与管理评审的实施情况	• 涉及标准的安全要素; • 受审核方的所有部门
审核报告	• 第一阶段的审核结论主要是对体系策划的充分性、风险评估和法律要求符合的充分性,以及体系文件的符合性进行评价	• 整个审核的结论,对体系的符合性、有效性与适应性进行全面评价

2）第二阶段的现场审核

工作内容包括：首次会议；现场检查、收集审核证据；内部评定,由审核组汇总分析审核证据结论,被审核申请方不参加内部评定；末次会议,审核组向被审核的组织领导包括信息安全管理经理等,报告审核过程总结情况、发现的不符合项、审核结论、现场审核结束后的有关安排等,主要有以下内容：

（1）审核范围的再次确认。

（2）不符合项的概要,纠正措施要求。

（3）任何观察资料及建议性活动的概述。

（4）审核的综合评论。

（5）宣布审核结论建议。

（6）建议或认证的其他方面。

（7）审核机密性的再次确认。

审核的期限取决于但并不局限于下列因素；

（1）要面谈的人员的数量。

（2）所持的数据量。

（3）地点的数目。

（4）与外界的接口。

（5）使用的信息技术的复杂度。

（6）组织是否已经有了相关鉴定的管理系统证书。

（7）业务功能。

（8）行业类型。

（9）风险程度。

3）编制审核报告

现场审核后，审核组应编制审核报告，做出审核结论。审核组将审核报告提交认证机构、申请方等。审核报告包括以下方面：

（1）审核场所。

（2）组织及适用的 ISO/IEC 27001 控制要求，参阅审核计划与适用性声明。

（3）组织关键文件的发布日期与版本，包括：方针、策略、程序、范围、适用性声明等文件。

（4）适用于组织的额外的强制性或自愿性标准或规则。

（5）审核结果的综合评论。

（6）不符合项和观察报告的编号识别及类别。

（7）审核涉及的人员。

审核结论有以下三种情况：

（1）信息安全管理体系已建立，运行有效，无严重不符合项和轻微不符合项，同意推荐认证通过。

（2）信息安全管理体系已建立并正常运行，在审核过程中发现少数轻微不符合项或个别严重不符合项，要求组织在规定的时间内实施纠正措施，同意在验证纠正措施的实施后推荐认证通过。

（3）信息安全管理体系仍有缺陷，在审核过程中发现较多的不符合项，需要在实施纠正措施后安排复审，本次不予以推荐认证通过。

8.3.3　证书与标志

组织采取了必要的纠正措施之后，并由认证机构验证通过，认证机构将为组织颁发 ISMS 证书，证书包括的内容如下：

（1）组织全称，涉及的相关组织。

（2）业务的相关地点。

（3）业务的流程。

（4）相关的业务功能与活动。

（5）认证的范围。

（6）适用性声明和特定版本的描述。

（7）关于信息安全系统满足 ISO/IEC 27001 认证标准的声明。

（8）证书开始生效的时间。

（9）证书号。

只有认证机构认可了组织的认证范围，才能在证书上显示认可标志。

8.3.4　维持认证

审核和证书颁布并不代表认证结束。通过执行每年至少一次的监督审核，认证机构将继续监控 ISMS 符合标准的情况。这些监督审核的重点是抽样检查系统的某些领域，所以

比最初的审核时间短，审核时间约为初始现场审核时间的三分之一。尽管审核团队可能会随时间不同而变化，但是对他们的能力要求和最初审核人员是一样的。

被认证机构有义务通知认证机构组织所发生的可能影响到系统或者证书的变更。这些变更包括：组织变更、人员变更、业务核心变更、技术变更、外部接口变更等。

认证的有效期一般为三年。三年之后，系统需要认证机构重新进行审核。

对于被认证组织而言，认证后要定期进行自我评估活动，监控和检查 ISMS，包括：

（1）检查 ISMS 的范围是否充分。

（2）进行定期 ISMS 有效性检查。

（3）进行定期的规程文档的审查，以实施 ISMS。

（4）审查可接受的风险水平，考虑组织变更、技术、业务目标的变化。

（5）实施 ISMS 的改善。

（6）采取适当的校正或者预防行动。

思考题

1. 论述信息安全管理体系认证的目的和作用。
2. 拟定信息安全管理体系认证范围需考虑哪些因素？
3. 叙述信息安全管理体系认证的基本条件。
4. 论述信息安全管理体系的认证过程。
5. 试述信息安全管理体系认证第一阶段与第二阶段审核的差异。
6. 归纳信息安全管理体系认证审核报告的主要内容。

第9章 信息安全管理控制措施

所有类型的组织，不管其规模大小，都有保护信息资产安全的需求，这些安全需求来源于以下各个方面：组织的业务特征、组织如何规划业务、业务流程、所使用的技术、业务合作伙伴、服务和服务提供商、法律环境以及组织所面临的风险。

9.1 选择控制措施的方法

1. 选择控制措施的原则

选择控制时，组织应当建立一套标准，指导在可选与备选控制措施中选择最佳控制措施来满足安全需要。这种标准要包括所有的限制条件和限制因素，其对决策有重要影响。组织采用什么样的方法来评估安全需求和选择控制措施，完全由组织自己来决定，但无论采用什么样的方法、工具，都需要对安全需求进行评估，并逐一选择控制措施。

在法律需求、业务需求和风险评估结果基础上，确定并评估能满足这三种安全需求的控制措施，使这些控制措施与业务环境保持一致，并能应对可能出现的后果，要求选择的控制措施最好地满足相关业务准则。

2. 影响选择控制措施的因素和条件

1）成本

在选择安全控制措施时，有大量的与成本有关的因素要考虑，控制措施的选择要基于安全平衡的原则，要考虑技术的、非技术的控制因素，也要考虑法律、法规的要求、业务的需求以及风险的要求。组织应该寻求在某些地方使用一些有效的、廉价的、非技术的措施以代替技术性的措施，用尽量少的控制措施、完成更多的控制目标，这样可以降低控制成本。

市场上有大量的安全产品可以实现特定的安全需要，为了更有效地进行选择，可以采用检查列表的方式，列出系统所需的最小安全保证、成本、可用性、安全因素等内容，逐项检查筛选，以保证所选择的安全产品既能提供所需的安全，又能限制在一个合理的成本范围内。

如果控制措施的成本大于其要保护的资产的价值，这种安全控制措施就失去意义了；安全的投入最好也不要超过组织所给定的预算额度。实施信息安全，也要计算投资回报，要有经济的概念。

为了降低成本，有些风险可以不采用控制措施。对于一个组织来说，不实施控制措施的

风险，意味着组织可以接受这种风险，但对于信息安全的实施者来说，不要忽视这些风险，要经常监视，确保这些风险的水平保持在组织可以接受的范围内。

2）可用性

在使用所选择的控制目标与控制措施时，可能会发现有些控制措施由于技术的、环境的原因，实施与维护起来很困难，或者根本就不可能实施与维护；同时，有些控制措施从用户的角度来看，如果存在不可操作或无法接受的一面时，也是不可行的。对于这些问题，信息安全的实施者一定要清楚，并找到相应的替代措施，例如非技术类的措施：物理、人员、过程的控制措施来补偿所需的技术控制，或作为技术控制的备用项。

有时系统所需的技术控制措施在市场上找不到合适的产品，这时可以考虑用相近产品来替代，但要考虑是否要加入补偿性措施，例如：相应的过程控制。

如果系统所需的技术控制措施在市场上找不到合适的产品，也没有相近产品来替代，这时组织就需要决定暂时接受这种风险，直到找到应对措施为止。

在选择所需的控制措施时，可以制定相应的安全架构设计，从而找到安全问题的对策。这些安全对策要与组织的信息技术架构相适应，保证实施的安全控制措施的兼容性与一致性，也便于日后的管理维护。

3）实施与维护

在选择控制时，要考虑实施与维护的简易性、成本、时间因素。如果在实施和维护一个控制措施时存在很大的困难，或者其成本、投入的人力过高，就要考虑寻找替代控制。例如，由于组织内部技术环境的限制，一个理想的技术控制很难实施，这时就要寻找相近的技术控制措施或者补偿性的过程控制措施来替代；又如，如果很难安全地实施远端系统维护，那么到用户现场来进行实地维护就是一个替代性的控制措施。

一旦确定了安全控制措施与合适的安全产品，就要在信息安全政策和实施计划中记录下来，并得到管理层的批准。应该尽可能快地实施，以免安全事件和事故的发生，实施时要尽量不影响用户工作与正常的业务运营，如果可能，最好安排在非工作时间。

实施完成后，就应该立即进行安全审计或符合性检查，以保证所需要的控制已正确实施，并可以有效地使用，相关测试也正确；如果有任何不足，要尽快弥补。

只有当所有的控制措施都已成功实施时，才能正式地接受并记录在案。对安全状态的维护应当定期进行，包括审计踪迹检查和分析、安全变更管理、安全事故处理等内容。

在实施与维护时，有一点是不能遗忘的，就是要对用户进行安全意识教育和技能培训。如果用户不知道安全为什么要维护，以及如何维护，那么再好的安全方案也发挥不了作用，相反，安全事故、安全侵害会接踵而至。

4）已存在的控制

控制措施的选择应当和组织中已经存在的控制措施有机地结合起来，共同为实现安全目标服务。对于组织中已经存在或已经计划的控制措施按以下情况进行检查：

（1）组织中已存在的控制措施可以提供足够的安全。在这种情况下，不需要再选择控制措施，如果要选择也只是为了将来的需要做准备。

（2）组织中已存在的控制措施不能提供足够的安全。在这种情况下，组织就需要做出决策：是否取消已有的控制或者是补充现有的控制。这种决策依赖于几个因素：控制成本的大小、更新是否必需、安全的需要是否迫切等。

组织还应该检查所选择的控制措施能否与现有控制相兼容。例如，物理访问控制可以用来补充逻辑访问控制机制，二者的结合可以提供更可靠的安全；对全体员工进行安全意识的教育可以保证员工能理解安全控制措施，并能在日常业务工作中正确地实施。

5）所有的控制目标与安全需求是否已满足

在最终决定实施安全控制措施之前，组织应当保证选择的控制措施可以满足所有的控制目标与安全需求。

需要指出的是，追求“零”风险是不切实际的，无论采取什么样的控制措施，总是存在剩余风险，问题是，对于这些剩余风险，组织能否接受？

首先，组织应该评估所选择的控制措施减轻了多少风险，然后决定哪些剩余风险是可以接受的，哪些剩余风险是组织无法接受的。这种决策要应用于整个组织范围内，以保证安全水平的连续性与一致性。如果一个或多个风险不能被组织接受，那么组织要考虑进一步采取控制措施。

在多数情况下，组织应当选择不同的控制措施来将风险降低到组织可以接受的水平，但选择的控制措施有时会导致过高的成本，有时会无法实施。例如，一个组织要应用电子商务与客户或业务伙伴进行贸易，面临的风险是财务信息有可能被损坏或篡改，这种风险对组织来说是不可接受的，唯一的控制手段是应用加密技术。如果这个组织的一个业务伙伴来自另一个国家，在那个国家不允许使用加密手段，那么保护措施就无法实施，其没有保护的电子商务所带来的相关风险组织是无法接受的。那么组织只能有两种选择，要么接受这种风险，要么不与业务伙伴进行交易。

所以，当不可能减少一种风险时组织就需要做出决策：接受风险还是采取其他行动。无论采取什么样的控制措施，最终结果只能是降低风险到可以接受的水平，或做出正式的管理决策接受风险。当然，也可以做出补充计划说明当这些风险发生时，如何采取补救措施以减弱负面影响。

9.2　选择控制措施的过程

安全措施的选择首先应考虑确定安全需求，然后通过一系列相关的决策过程决定选择什么样的控制措施。图9-1给出了从安全问题到控制措施的循环过程，在组织安全方针的指导下，从分析安全问题出发，明确安全需求，确定具体的安全控制目标，选择安全措施，以解决安全问题。

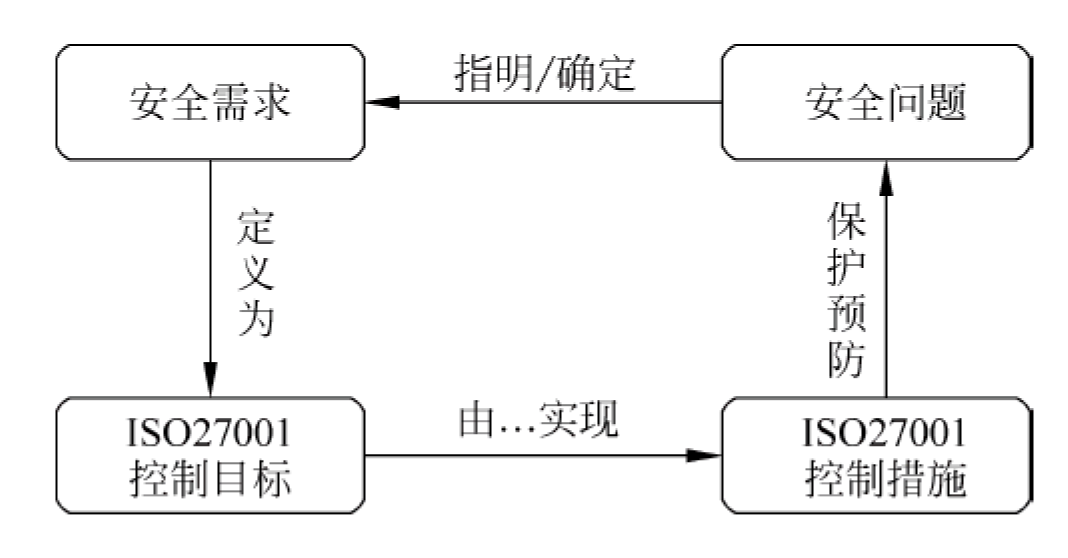


图9-1　选择安全控制的过程

安全需求与控制措施选择的关系如图 9-2 所示。遵守法律法规的要求是组织正常运营的基本要求，通常是一种强制性要求。组织应保证一切活动都要符合相应的法律法规的要求，以避免违法活动带来的诉讼风险。根据业务活动本身的特点来选择安全控制措施是一种最直接的方式，并与组织的业务特性紧密地结合在一起，所考虑的控制方式应能满足业务机密性与可持续性。通过详细的风险分析，可以确定组织所面临的各种主要风险，通过引入适当的控制，使风险降低到组织可以接受的程度，以满足组织提出的安全需求。

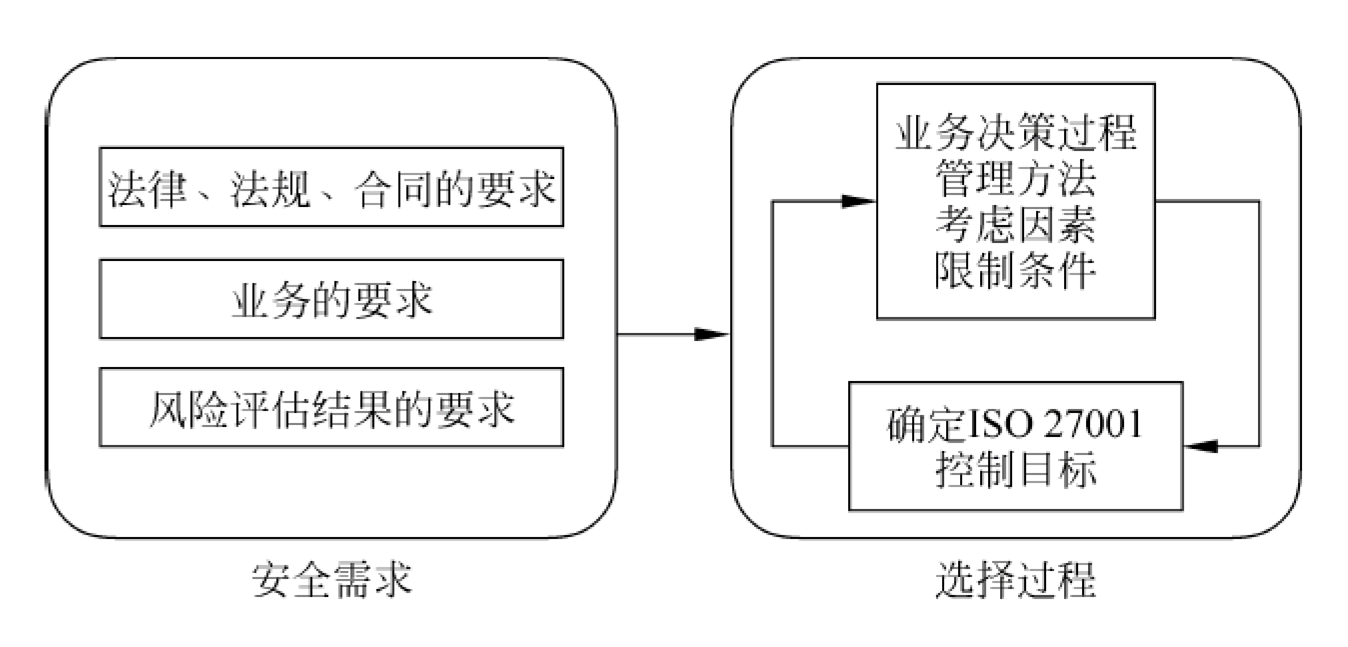


图 9-2　安全需求与控制选择

选择控制目标与控制措施时没有一套标准与通用的办法，选择的过程往往不是很直接，可能要涉及一系列的决策步骤、咨询过程，要和不同的业务部门和大量的关键人员进行讨论，对业务目标进行广泛的分析，最后产生的结果要很好地满足组织对业务目标、资产保护、投资预算的要求。正如前面章节所介绍，选择控制目标与控制措施可以基于与安全需求相关的各种因素，例如，选择的标准可以基于对威胁、脆弱性以及可能产生的风险的评估，也可以基于其他因素，如法律与业务的需求。

图 9-3 给出了选择控制措施的具体步骤。

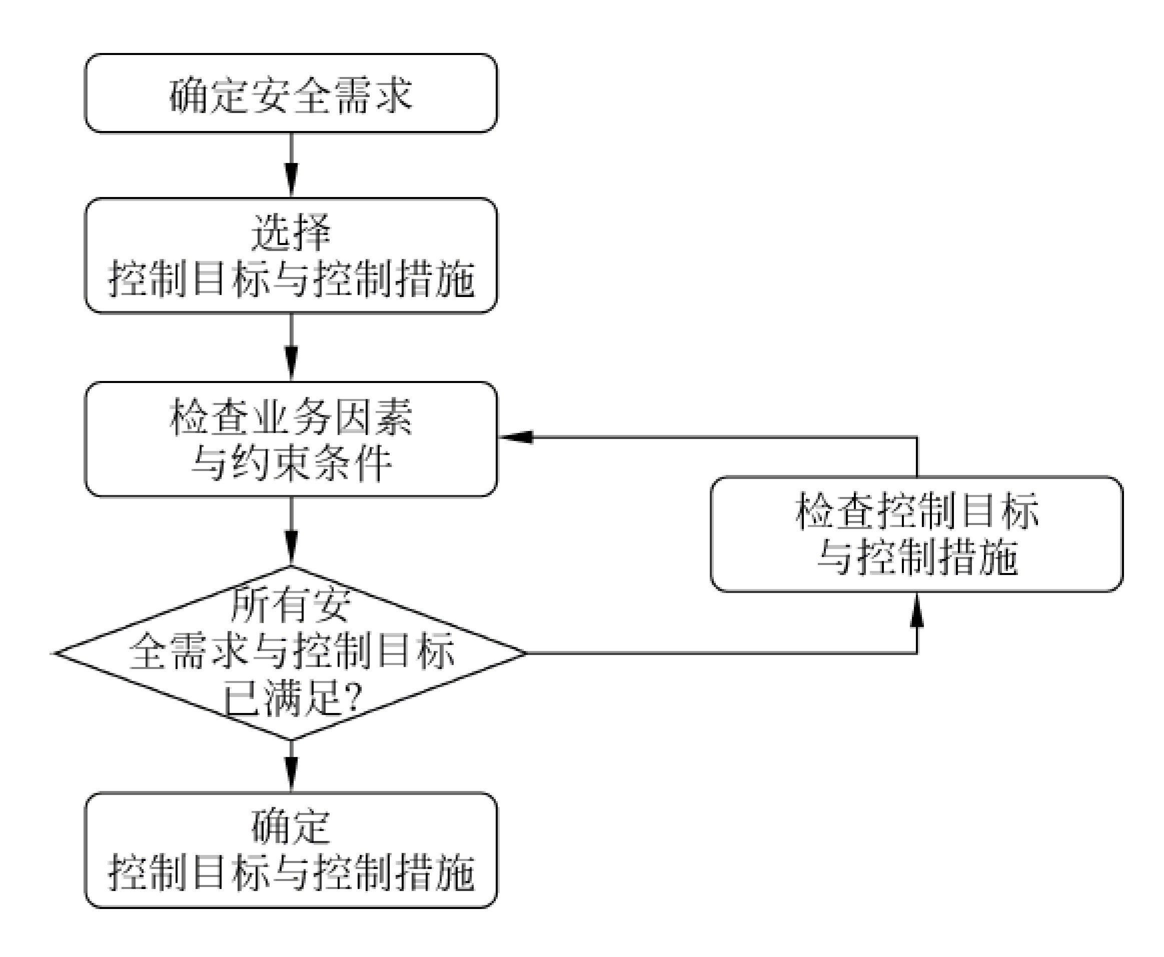


图 9-3　选择控制措施的过程

(1) 先考虑基于法律与业务的安全需求，可以从标准中选择符合法律和业务要求的相关控制目标和控制措施。

(2) 再考虑基于风险分析的安全需求，风险分析可以揭示组织中信息资产的脆弱性与

面临的威胁,通过评估风险的等级,从标准中选择相关控制目标和控制措施来防止威胁,弥补脆弱性,从而降低风险。

(3) 通过考虑各种安全问题,可以进一步完善和拓展所选择的控制目标和控制措施。

一般来说,如果用户有明确的安全需求,可以选择相关控制措施来满足法律与业务的安全需求,保护信息资产不受已有的风险的影响;通过检查安全问题,可以进一步完善控制目标和控制措施,使其更好地满足安全需求。用户根据实际情况,不使用其中的某些控制措施或增加其中没有涉及的控制措施,需要在适用性声明中加以说明。

9.3　风险管理

1. 确定安全需求

对控制目标与控制措施的选择应当由安全需求来驱动,选择控制措施应当是基于能最好地满足安全需求,并考虑安全需求得不到满足的后果。安全需求描述了组织信息安全的目标与需求,这种目标与需求的满足可以保证组织安全、成功地实现其业务目标。组织的安全需求一般来自以下三个方面的考虑:

1) 来自法律、法规、合同的需求

组织所处的内外环境都要求遵守法律法规、组织内部的规章制度以及与第三方签署的合同的约束。

2) 来自业务需求

组织制定和实施信息系统,是为了支持组织的业务运营,而组织为保证业务流程、业务目标的安全性、完整性、可用性,对信息安全提出了一定的要求。

3) 来自风险的安全需求

由于组织所处的环境以及信息处理设施都存在一定的薄弱性,信息资产的薄弱点被威胁利用就会产生风险,并可能对业务产生一定的影响与损害。

2. 风险评估与风险管理

风险评估和风险管理的过程是组织确定安全需求的重要一环。在确定风险、管理风险、选择控制目标与控制措施降低风险的过程中,组织应当在业务上考虑各种经济的、业务的、法律的约束条件。通过详细的风险分析,可以确定组织所面临的各种主要风险,通过引入适当的控制,将风险降到组织可以接受的程度,就可以满足风险所提出的安全需求。

了解组织信息安全需求的最主要的方式就是实施风险评估,对信息资产评估风险以后,组织能够:

(1) 评审风险的后果,评审安全事件的发生会对组织的业务有什么样的影响与损害。

(2) 对怎样管理风险做出决策,包括接受风险、避免风险、转移风险、降低风险。

(3) 采取相应的措施来实施风险管理决策和控制措施。

3. 风险管理的方法

在风险评估的基础上建立信息安全管理体系,进行风险的处理和控制措施的选择。法

律需求与业务需求是整个控制选择过程的重要内容,不可忽视,处理风险的方法同样适用于法律需求与业务需求对控制措施的要求。

1) 接受风险

对风险评估确定的风险可以通过 4 种方法进行管理,第一种方法就是决定是否在某一点上接受风险,不做任何事情,不引入控制措施。但是一般还是推荐采取一定的措施来避免安全风险产生安全事故,防止由于缺乏安全控制而对正常业务运营造成损害。

如果认为风险是组织不能接受的,那么就需要考虑其他三种方法来应对某个风险或某些风险,这三种方法如图 9-4 所示。

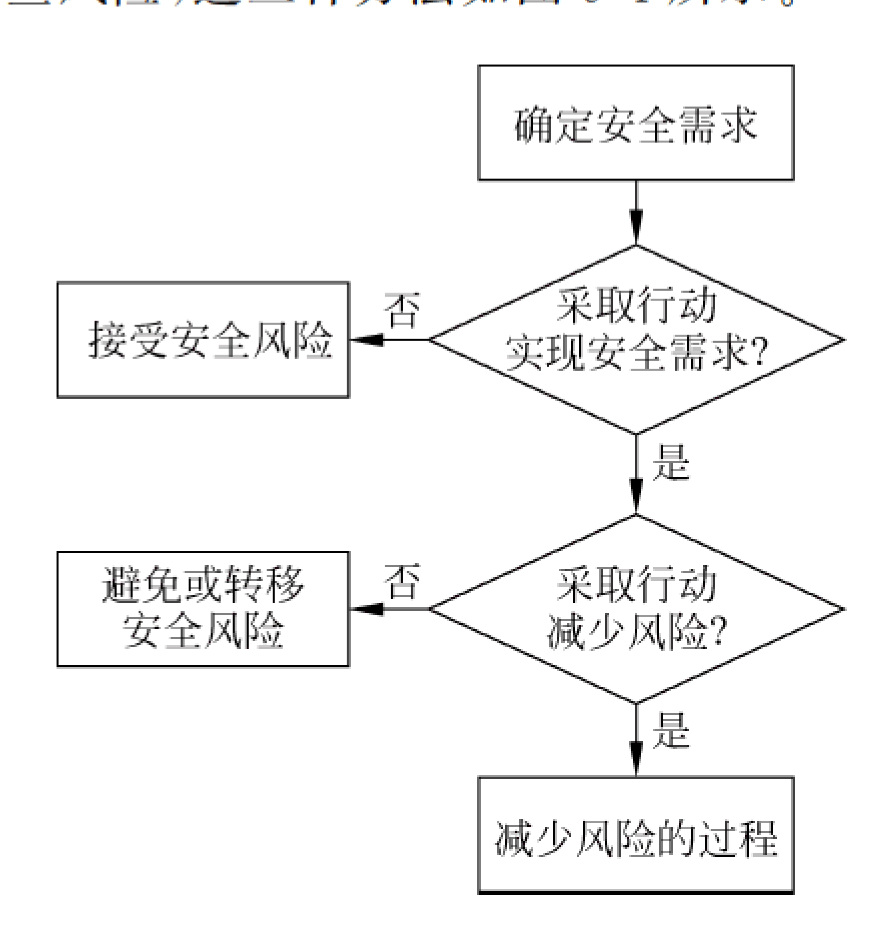


图 9-4 风险管理的方法

2) 避免风险

避免风险是组织决定绕过风险,例如,通过放弃某些业务活动或主动从风险区域撤离来避免风险。采取避免风险的措施时,需要在业务需求与资金投入方面进行权衡。尽管有黑客的威胁,由于有业务的需求,组织不可避免地要使用 Internet,这时可以考虑降低风险的方式;把整个组织撤离到安全场所可能会需要巨大的投入,这时可以考虑采用风险转移的方式。

3) 转移风险

转移风险是组织无法避免风险时的一种可能的选择,或者是在减少风险很困难、成本很高时,组织采取的一种方法。例如,对已经评估确认的价值较高、风险较大的资产进行保险,把风险转移给保险公司。

另一种转移风险的方式把关键业务处理过程外包给专业的第三方组织,因为他们拥有更好的设备、高水平的专业人员。这时,要考虑的是要在与第三方签署的服务合同中详细描述所有的安全需求、控制目标与控制措施,以确保第三方提供服务时也能提供足够的安全。尽管这样,在许多外包项目的合同条款中,外购的信息及信息处理设施的安全责任大部分还是落在组织自己身上,对于这一点要有清醒的认识。

还有一种转移风险的方式是把要保护的资产从信息处理设施的风险区域转移出去,以减少对信息处理设施的安全要求。例如,一份高度机密的文件使得存储与处理此文件的网络的风险变得格外突出,如果把这份文件转移到单独的 PC 上,那么网络的风险就变得不那么突出了,也更容易处理了。

4) 降低风险

所谓降低风险就是通过选择控制目标与控制措施来降低评估确定的风险。结合下列各种控制措施来降低风险,达到可以接受的安全水平:

(1) 减轻威胁——减少威胁出现的可能性。

(2) 减少脆弱性——减轻并弥补系统脆弱性。

(3) 降低影响——把安全事件的影响降低到可接受的水平。

(4) 检测意外事件。

(5) 从意外事件中恢复。

这样就可以保证各种控制措施之间相互补充、相互支持，例如，技术控制与过程控制结合使用可以使两者更有效。

在选择控制时，组织应当建立一套标准，指导在可选与备选控制中选择最佳控制来满足安全需要。这种标准要包括所有的限制条件和限制因素，因为这对选择的决策有重要影响。

组织采用什么样的方法来评估安全需求和选择控制，完全由组织自己来决定，但无论采用什么样的方法、工具，都需要对前面所描述的三种安全需求进行评估，并逐一选择相关控制。

在法律需求、业务需求和风险评估结果基础上，选择控制的过程应当：

(1) 确定与评估能满足这三种安全需求的控制，使这些控制与业务环境相称，并能应对可能出现的后果。

(2) 选择的控制要能最好地满足相关业务准则。

9.4　信息安全管理控制规范

9.4.1　从需求解析信息安全管理控制措施

1. 法律需求

根据 ISO/IEC 27001 第 A.15.1.1 项的要求，组织必须确定适用的法律、法规与标准并记录在案、保持更新，这种要求可以由 ISO/IEC 27001 的控制措施来实现，表 9-1 描述了 ISO/IEC 27001 中第 15 条款所定义的法律的要求及其相关控制措施的示例。这个表不一定适合每个组织的情况，组织可根据自己的业务目标与业务特点追加适合自己的法律、法规、标准的要求。(本节以下各表中省略了 ISO/IEC 27001 标准附录的 A. 标号。)

表 9-1　安全需求与相关控制

需　　求	相关控制措施
可用的法律识别	5.1.1、5.1.2、6.1.1、7.2.1、8.1.1、8.1.2、8.1.3、13.2.2、15.1.1
知识产权	5.1.1、5.1.2、6.2.2、6.2.3、8.1.1、8.1.3、8.3.1、8.3.2、10.2、10.8.2、11.6.1、12.4.1、12.4.3、12.5.3、12.5.5、15.1.2、15.2.1、15.3.2
保护组织的记录	5.1.1、5.1.2、6.1.3、6.1.5、7.1.3、7.2.2、8.1.3、8.2.2、8.2.3、10.1.1、10.2.2、10.10、11.1.1、11.2.1、11.2.4、11.5.1、11.5.2、11.5.4、11.6.1、12.1.1、12.3.1、12.5.1、15.1.3、15.2.1
密码控制措施的规则	5.1.1、6.1.1、6.1.3、10.8.1、10.9、12.3、15.1.6

2. 业务需求

组织的业务需求来源于与信息处理相关的业务目标、业务标准和业务流程，每一个组织的需求都有其特点，但还是存在一些通用的需求，表 9-2 列出了 ISO/IEC 27001 中所支持的、与较为通用业务需求内容相应的主要控制措施示例。

表 9-2 部分通用业务需求与相关控制

需　　求	相关控制措施
外包与第三方供应商	6.2.1、6.2.3、10.2、10.6.2、10.8、11.4.6、11.6.1、12.5.3、12.5.5
符合标准与安全政策	5.1.1、5.1.2、6.1.3、6.1.5、8.1.1、8.1.3、10.1.1、10.2.1、10.9、13.1.1、13.2.3、14.1、15.1、15.2
与安全活动相协调	5.1、6.1.2、6.1.6、6.1.7、6.2.2、6.2.3、10.2、10.6.2、13.1.1、13.2.3
正确的业务处理流程	6.1.4、7.2.2、8.2.2、10.1.1、10.1.2、10.2.3、10.6.2、10.8.5、10.10.2、11.1.1、11.2.1、11.2.3、12.5.1、13.1、13.2.1、13.2.2、15.3.1、15.3.2
信息与信息处理设施的可用性	6.1.4、7.1.2、7.1.3、9.1.3、9.2.1、9.2.5、9.2.6、10.3.1、10.5.1、10.7.3、10.8.5、11.6.1、12.4.1、15.2.2

3. 风险评估的需求

为了实现组织的安全需求，可以通过风险评估确定引起风险的原因所存在的方面：资产、威胁及脆弱性。ISO/IEC 27001 列出了典型的威胁和脆弱性，并列出相应的控制措施来应对威胁、减轻脆弱性。

表 9-3 抽取部分 ISO/IEC 27001 所涉及的安全内容与范围、列出了在各种组织中常见威胁和脆弱性的示例。有些在组织、业务伙伴或贸易环境中可能出现的威胁和脆弱性，可能没有包含在列表中，组织可以自己识别出来，并找到相应的控制措施。

表 9-3 风险评估的需求与相关控制

需　　求	相关控制措施
安全侵害	
缺乏有安全政策而造成的安全侵害	5.1.1、5.1.2、6.1.1、6.1.3、6.2.3、8.1.1、8.1.3、8.2.1、10.8.1、13.2.1、15.2.1
缺乏安全意识而造成的安全侵害	5.1.1、5.1.2、6.1.1、8.2.2、10.4.1
缺乏安全组织与协调机构而造成的安全侵害	6.1.1、6.1.2、6.1.6、6.1.7、6.2.2、6.2.3、10.2.2、13.1.1、13.2.2
非授权变更	
非授权的软件安装或软件变更	6.1.4、10.1.2、10.2.1、10.2.3、12.5.1、12.5.3
信息处理设施的非授权变更	6.1.4、6.2.3、8.3.3、10.1.2、12.5.1、12.5.2
对测试、开发及运行设施的滥用	6.1.4、7.1.2、10.1.1、10.1.4、10.3.1、11.5.4、15.1.5
安全事件与故障	
安全事件重复出现造成的损害	5.1.1、6.1.3、10.5.5、13.1.1、13.1.2、13.2.2
软件故障造成的损害	6.1.2、6.2.1、10.1.4、10.2.1、12.4.3、12.5.3
系统失效	10.3.1、10.3.2、10.8.5、10.10.2、12.1.1、14.1.1、14.1.3、14.1.5

9.4.2 从安全问题解析信息安全管理控制措施

表 9-4 举例描述了 ISO/IEC 27001 附录 A 控制 5.1 所关注的相关安全问题，通过实施这种控制措施可以防止此类安全问题的发生。此外，此表还描述了安全问题会损害资产的哪一种特性(机密性－C，完整性－I，可用性－A，法律、法规、合同的要求－L)。

表 9-4　与信息安全政策文件相关的安全问题示例

安全问题	对资产特性的威胁
因为员工不了解或误解安全政策而造成的安全损害(例如,违反法律、标准、安全政策、病毒处理措施、业务连续性计划等行为)	C、I、A、L
由于缺乏合理的报告机制致使安全事故重复出现造成的安全损害	C、I、A、L
由于员工不了解安全的重要性而造成的安全损害(包括有意的破坏或意外事故)	C、I、A、L
由于缺乏管理层的支持而造成的安全损害(例如,为安全而分配的资源不足时易发生的损害)	C、I、A、L

9.4.3　控制目标与控制措施详述

国家标准 GB/T 22080—2008 附录 A 涉及信息安全管理的 11 个领域,共列出了 39 个控制目标和 133 项信息安全控制措施,见表 9-5。这些控制措施汇集了信息安全管理的最佳实践,组织应根据信息安全风险评估结果并结合组织的内部和外部的环境,以及整体业务要求从中进行选择,当然也可以根据组织的实际情况选择其他控制措施。

对风险的管理过程如图 9-5 所示。

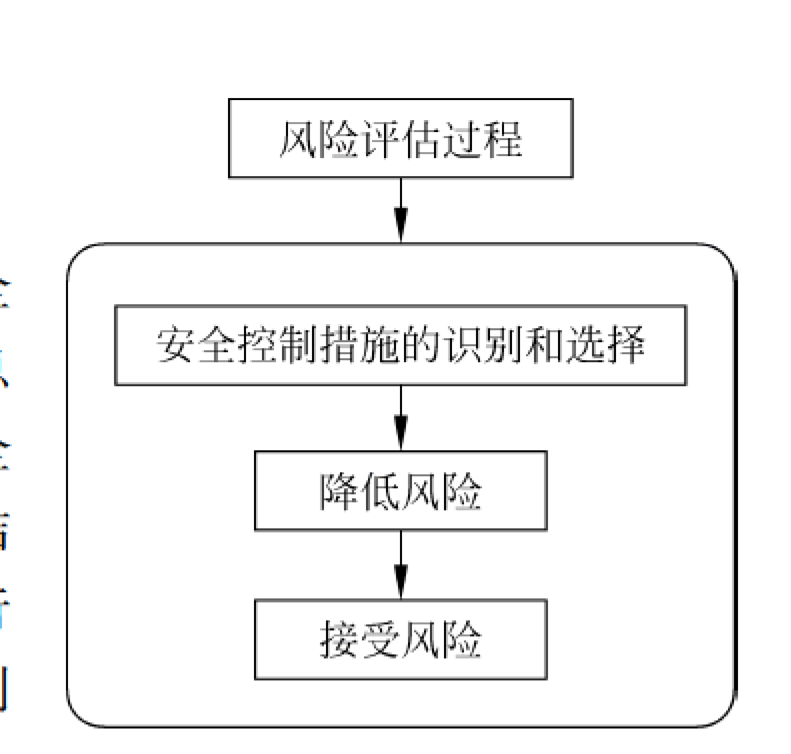


图 9-5　风险管理过程

表 9-5　ISO/IEC 27001 133 项控制措施

11 个方面 133 项信息安全控制措施			
ISO/IEC 27001 附录 A	信息安全控制措施域	控制目标	控制措施
A5	安全方针	1	2
A6	信息安全组织	2	11
A7	资产管理	2	5
A8	人力资源安全	3	9
A9	物理和环境安全	2	13
A10	通信和操作管理	10	32
A11	访问控制	7	25
A12	信息系统获取、开发和维护	6	16
A13	信息安全事件管理	2	5
A14	业务连续性管理	1	5
A15	符合性	3	10
合　计		39	133

1. A.5　安全方针

A.5.1　信息安全方针

目标:依据业务要求和相关法律法规提供管理指导并支持信息安全。

内容解析:在建立并保持信息安全方针时需依据业务要求和相关法律法规要求,确保

信息安全方针得到最高管理者的支持，使所有相关的人员（内部或外部的）了解其关于信息安全的责任。

A.5.1.1　信息安全方针文件

控制措施：信息安全方针文件应由管理者批准、发布并传达给所有员工和外部相关各方。

内容解析：通过安全方针建立全体员工的信息安全意识并支持组织的业务运行与发展。信息安全方针可以形成一份单独的文件，由组织的高级管理者签署批准，在组织内以可访问的方式发布。信息安全方针是组织安全管理的指导性文件，其他安全管理策略、过程和规程等应与信息安全方针保持一致。

A.5.2　信息安全方针的评审

控制措施：应按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保它的持续性和适宜性、充分性和有效性。

内容解析：组织的环境和业务状况等处于变化中，应按组织预定的周期对信息安全方针进行评审；或者当发生对信息安全产生影响的重大事件时对安全方针进行评审。根据评审结果对信息安全方针加以必要修订，以适应业务环境的变化和组织安全管理的需要。

2. A.6　信息安全组织

A.6.1　内部组织

目标：管理组织内部的安全。

内容解析：应建立管理框架，以启动和控制组织范围内的信息安全的实施。

管理者应批准整个组织内的信息安全方针、分配安全角色并协调和评审安全的实施。若需要，要在组织范围内建立信息安全专家建议的资料源，并在整个组织内均可获得该资料。要发展与外部安全专家或组织（包括相关权威人士）的联系，以便跟上行业发展趋势、跟踪标准和评估方法，并且当处理信息安全事故时，提供合适的联络地点。应鼓励信息安全的多学科交叉途径。

通过高层管理者的支持和协调，基于组织的文化、业务目标和要求在组织内实施信息安全管理。

A.6.1.1　信息安全的管理承诺

控制措施：管理者应通过清晰的方向、说明性承诺、明确的信息安全职责分配和确认，来积极地支持组织内的安全。

内容解析：管理承诺体现了高层管理对信息安全管理的领导力。

- 实施指南

管理者应：

a）确保信息安全目标得以识别，满足组织需求，并已被整合到相关过程中；

b）制定、评审、批准信息安全方针；

c）评审信息安全方针实施的有效性；

d）为安全举措提供清晰的方向和可视化的管理者支持；

e）为信息安全提供所需的资源；

f）批准整个组织内信息安全特定角色和职责的分配；

g）启动计划和程序来保持信息安全意识；

h）确保整个组织内的信息安全控制措施的实施相互协调；（见 A.6.1.2）。

管理者应该根据专家的建议，区分内部和外部需求，并且在整个组织范围内评审和协调建议结果。

根据组织的大小，这些职责可以由一个专门的管理协调小组或由一个已存在的机构承担，例如董事会。

A.6.1.2　信息安全协调

控制措施：信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调。

内容解析：信息安全工作需要在各部门或不同的领域间协调，有关信息安全的考虑和工作应有一种沟通及驱动机制，如建立跨部门的协调机构或安全负责人会议。协调程度与组织的规模有关联，对于一个小型组织可能没有明确的协调组，关键点是规定责任人。

• 实施指南

典型地，信息安全协调应包含管理人员、用户、行政人员、应用设计人员、审核员和安全专员，以及各领域专家技术的协调和协作，这些领域包括保险、法律问题、人力资源、IT 或风险管理等。这些活动应：

a）确保安全活动的实施与信息安全方针相一致；

b）确定如何处理不符合；

c）核准信息安全相关的方法和过程，例如风险评估、信息分类；

d）识别重大的威胁变化和信息系统内暴露于威胁下的信息和信息处理过程；

e）评估信息安全控制实施的充分性和协调性；

f）有效地促进整个组织内的信息安全教育、培训和意识；

g）评价在信息安全事故的监视和评审中获得的信息，推荐适当的措施响应识别的信息安全事故。

如果组织没有使用一个独立的跨部门的小组，例如因为这样的小组对组织规模来说是不适当的，那么上面描述的措施应由其他的合适的管理机构或单独管理人员实施。

A.6.1.3　信息安全职责的分配

控制措施：所有的信息安全职责应予以清晰地定义。

内容解析：信息安全的职责应在组织内分配并针对所涉及的岗位以书面的方式做出规定（如岗位职责说明）。安全管理职责的规范应从最直接的角色作为起点并扩展到相关层面的岗位。

• 实施指南

信息安全职责的分配应和信息安全方针相一致。各个资产的保护和执行特定安全过程的职责应被清晰地识别。这些职责应在必要时加以补充，来为特定地点和信息处理设施提供更详细的指南。资产保护和执行特定安全过程（诸如业务连续性规划）的局部职责应予以清晰地定义。

分配有安全职责的人员可以将安全任务委托给其他人员。虽然如此，他们仍然负有责任，并且他们应能够确定任何被委托的任务是否已被正确地执行。

个人负责的领域要予以清晰地规定，特别是，应进行下列工作：

a）与每个特殊系统相关的资产和安全过程应予以标识并清晰地定义；

b）应分配每一资产或安全过程的实体职责，并且应形成该职责细节的文件；

c）授权级别应清晰地予以定义，并形成文件。

在许多组织中，将任命一名信息安全管理人员全面负责安全的开发和实施，并支持控制措施的识别。

然而，提供控制资源并实施这些控制措施的职责通常归于各个管理者。一种通常的作法是对每一资产指定一名拥有者，他也就对该信息资产的日常保护负责。

A. 6. 1. 4　信息处理设施的授权过程

控制措施：应规定并实施新信息处理设施的管理授权过程。

内容解析：对于新的信息处理设施（包括个人的信息处理设备）或更新的设备进入组织的网络和业务环境，管理层应制定并发布一个正式的授权过程，向下可贯彻到部门级。授权应在运行管理和技术两方面把控。

- 实施指南

授权过程应考虑下列指南：

a）新设施要有相应用户管理者的授权，以授权设施的用途和使用；还要获得负责维护本地系统安全环境的管理者授权，以确保所有相关安全策略和要求得到满足；

b）若需要，硬件和软件应进行检验，以确保它们与其他系统部件兼容；

c）使用个人或私有信息处理设施处理业务信息，可能引起新的脆弱点，因此应识别和实施必要的控制。

A. 6. 1. 5　保密性协议

控制措施：应识别并定期评审反映组织信息保护需要的保密或非扩散协议的需求。

内容解析：组织应按适用的法律规定编制保密协议或不泄密协议并在一定范围内要求相关人员签署，以保护机密信息。管理层应咨询内部或外部的法律专家或顾问以确保这种类型的协议是恰当准确的，并反映了组织的要求。保密协议的要求应定期评审，以适应组织信息保护的需要。

保密协议可适用于内部人员或外部相关方及人员。

- 实施指南

保密或不泄漏协议应使用合法且可实施条款来解决保护机密信息的要求。要识别保密或不泄漏协议的要求，需考虑下列因素：

a）定义要保护的信息（如机密信息）；

b）协议的期望持续时间，包括不确定的需要维持保密性的情形；

c）协议终止时所需的措施；

d）避免未授权信息泄漏的签署者的职责和行为（即“需要知道的”）；

e）信息所有者、商业秘密和知识产权，以及他们如何与机密信息保护相关联；

f）机密信息的许可使用，及签署者使用信息的权力；

g）对涉及机密信息的活动的审计监视权力；

h）未授权泄漏或机密信息破坏的通知和报告过程；

i）关于协议终止时信息归档或销毁的条款；

j）违反协议后期望采取的措施。

基于一个组织的安全需求，在保密性或不泄漏协议中可能需要其他因素。

保密性和不泄漏协议应针对它适用的管辖范围（参见 A.15.1.1）遵循所有适用的法律法规。

保密性和不泄漏协议的要求应进行周期性评审，当发生影响这些需求的变更时，也要进行评审。

保密性和不泄密协议保护组织信息，并告知签署者他们的职责，以授权、负责的方式保护、使用和不泄漏信息。

对于一个组织来说，可能需要在不同环境中使用保密性或不泄密协议的不同格式。

A.6.1.6　与政府部门的联系

控制措施：应保持与相关政府机构的适当联系。

内容解析：政府部门指警方、消防、安全和司法单位等。组织应与本地的这些有关安全的部门建立并保持联系，以便确保能对负面或重大事件的发生做出快速响应。

• 实施指南

组织应建立程序，规定何时应当与哪个机构（例如，执法部门、消防局、监管部门）联系，如果怀疑已识别的信息安全事故可能触犯了法律，如何及时报告。

由于互联网而遭受攻击的组织可能需要外部第三方（例如互联网服务提供商或电信运营商）采取措施以抵制攻击源。

保持这样的联系可能是支持信息安全事故管理或业务连续性和偶然性规划过程的一个要求。与法规部门的联系也是有用的，以预测和准备即将到来的组织必须遵循的法律法规方面的变化。与其他部门的联系包括公共部门、紧急服务和健康安全部门，例如消防局、电信提供商（与路由和可用性有关）、用水供应者（与设备的冷却设施有关）。

A.6.1.7　与特定利益集团的联系

控制措施：应保持与特殊利益团体或其他专家安全论坛和行业协会的适当联系。

内容解析：组织内从事信息安全的人员应与信息安全相关的特定机构（如行业协会、安全监控中心等）建立联系，以便获得有关信息安全的动态信息并使之受益于本组织。

• 实施指南

获得特殊利益团体或论坛的成员资格，应考虑将其作为一种方式：

a）增进关于相关安全信息的最佳实践和最新状态的知识；

b）确保对于信息安全环境的理解是最新的和完整的；

c）尽早接受到关于攻击和脆弱点的警告、建议和补丁；

d）获得得到信息安全专家建议的途径；

e）分享和交换关于新的技术、产品、威胁或脆弱点的信息；

f）提供处理信息安全事故时的适应的联络地点（参见 A.13.2.1）。

建立信息共享协议来改进安全问题的协作和协调。这种协议应识别出保护敏感信息的要求。

A.6.1.8　信息安全的独立评审

控制措施：应按计划的时间间隔或当发生重大的信息安全变化时，对组织的信息安全管理方法及其实施情况（例如，信息安全控制目标、控制措施、策略、过程和程序）进行独立评审。

内容解析：独立评审指独立于评审范围而又具有一定信息安全管理经验、知识或技能的人员对组织信息安全管理所进行的评审。由于一个组织的信息安全管理资源的限制，执行独立评审的人员也可能来自于组织外部的专家或第三方人员。

为确保控制措施和安全防护的有效性和适用性，管理层应在计划的周期或当环境或业务运行发生较大变更时协调资源或结合内部审核对信息安全管理的实践（包括方针、控制目标、措施、过程和规程等的实施情况）进行评审。这里是否需要调集外部资源（例如，评估师或审核员）需要管理层做出决策，评判依靠组织内部的安全审核是否已经足够。

- 实施指南

独立评审应由管理者发起。这种独立评审对确保组织管理信息安全方法的持续适宜性、充分性和有效性是必需的。评审应包括评价安全方法改进的机会和变更的需要，包括策略和控制目标。

这样的评审应由独立于被评审区域的个人执行，例如内部审核部门、独立的管理者或专门做这种评审的第三方组织。从事这些评审的个人应具备适当的技能和经验。

独立评审的结果应被记录并报告给启动评审的管理者。这些记录应加以保持。

如果独立评审识别出组织管理信息安全的方法和实施不充分或不符合信息安全策略文件中声明的信息安全的方向，管理者应考虑纠正措施。

管理者应定期评审（A.15.2.1）的区域也要独立评审。评审方法包括访谈管理者、检查记录或安全策略文件的评审。ISO 19011：2002，质量和/或环境管理体系审核指南，也提供实施独立评审的有帮助的指导信息，包括评审方案的建立和实施。A.15.3 详细说明了与运行的信息系统独立评审相关的控制和系统审核工具的使用。

A.6.2　外部各方

目标：保持被外部组织访问、处理、沟通或管理的组织信息及信息处理设备的安全。

内容解析：组织的信息处理设施和信息资产的安全不应由于引入外部各方的产品或服务而降低。任何外部各方对组织信息处理设施的访问、对信息资产的处理和通信都应予以控制。若有与外部各方一起工作的业务需要，它可能要求访问组织的信息和信息处理设施、从外部各方获得一个产品和服务或提供给外部各方一个产品和服务，就要进行风险评估，以确定安全蕴涵和控制要求。在与外部各方签订的合同中要商定和定义控制措施。

为方便业务活动，外部相关方往往需要对组织的信息和信息处理设施进行访问，沟通信息并参与信息的处理，或许还有本组织的信息和信息处理设施处于外部方的管理之下，对此组织应有充分的安全准备，以确保信息和信息处理设施的安全。

A.6.2.1　与外部各方相关风险的识别

控制措施：应识别来自涉及外部组织的业务过程的信息和信息处理设施的风险，并在允许访问前实施适当的控制。

内容解析：在与外部组织合作开展业务前应识别信息安全风险，基于风险评估的结果，在合作业务运行前应安排并实施控制措施。

A.6.2.2　处理与顾客有关的安全问题

控制措施：应在允许顾客访问组织的信息或资产前强调所有的安全要求。

内容解析：在允许顾客访问组织的信息或资产之前，通过信息安全风险评估已经识别的风险应全部处理完成并验证满足要求。

A.6.2.3　处理第三方协议中的安全问题

控制措施：涉及访问、处理或管理组织的信息处理设施以及与之通信的第三方协议，或在信息处理设施中增加产品或服务的第三方协议，应涵盖所有相关的安全需求。

内容解析：外部第三方在访问、处理或交流组织的信息、访问组织的信息处理设施或在信息处理设施中增加产品或服务前要预先签订协议，其中应包含对信息安全的全部要求。可以就信息安全的要求单独签署协议，也可以将信息安全要求作为整个协议的组成部分。

3. A.7　资产管理

A.7.1　对资产负责

目标：实现并保持组织资产的适当保护。

内容解析：所有资产应是可核查的，并且有指定的责任人。对于所有资产要标识出责任人，并且要赋予维护相应控制的职责。特定控制的实施可以由责任人适当地委派别人承担，但责任人仍有对资产提供适当保护的责任。

基于对组织内全部资产的考察，落实对资产的安全责任，对有的资产需限定使用要求。对资产实施有针对性的保护，强化对重要和关键资产的保护。

A.7.1.1　资产清单

控制措施：应清楚识别所有的资产，编制并保持所有重要资产清单。

内容解析：组织应在与信息相关的全部资产中识别重要资产、列出清单并加以说明。资产清单要得到维护并在需要时进行更新。资产清单不仅是一份文件或是资产列表，其中应包括资产分类、保密级别、当前位置和责任人。信息安全管理可基于资产清单制定信息安全计划，对资产加以监控；资产清单还有助于在重大事件或灾后进行业务恢复。

A.7.1.2　资产责任人

控制措施：与信息处理设施有关的所有信息和资产应由组织指定的部门或人员承担责任。

内容解析：组织应结合信息处理环境指定资产的责任人。资产责任人对资产的使用、维护或信息的分发承担责任。

A.7.1.3　资产的可接受使用

控制措施：与信息处理设施有关的信息和资产的可接受的使用规则应被识别、形成文件并加以实施。

内容解析：组织内的人员需要使用组织提供的信息处理设施和信息以开展业务活动，但这些设施还可能被用来从事与组织业务无关的个人活动，如网上聊天、购物等。组织对与信息处理设施有关的信息和资产的使用要做出明确的规定，避免信息处理设施和资产被误用和滥用以致影响组织的正常业务运行。

A.7.2　信息分类

目标：确保信息可以得到适当程度的保护。

内容解析：应对信息进行分类，以在处理信息时指明保护的需求、优先级和期望程度。信息具有可变的敏感性和重要性。某些项可能要求附加等级的保护或特别的处理。信息分类机制用来定义一组合适的保护等级和传递特别处理措施的需求。

组织应建立信息的分类方案及保密等级，确保信息得到与其级别相适宜的保护。

A.7.2.1 分类指南

控制措施：应按照信息的价值、法律要求及对组织的敏感程度和关键程度进行分类。

内容解析：对信息和数据组织应基于其价值、关键性、敏感性、法律和业务要求划分保密类别，以便于对资产提供适当级别的保护。

A.7.2.2 信息的标记和处理

控制措施：应制定并实施一套与组织所采用的分类方案一致的信息标识和处置的程序。

内容解析：在信息和数据分类的基础上应制定信息的标记和处理规程。由于信息可以以物理和电子的方式储存，其标记需要针对不同的方式做出规定。例如，电子信息应采用电子标记的手段。信息处理规程旨在对各类级别保密信息的操作（包括安全处理、存储、传输、解密、销毁等）形成管理规范。分类信息的标记和处理是信息交流和共享的关键要素。

4. A.8 人力资源安全

A.8.1 任用之前

目标：确保员工、合同方和第三方用户了解他们的责任并适合于他们所考虑的角色，减少盗窃、滥用或设施误用的风险。

内容解析：安全职责应于雇用前在适当的岗位描述、雇用条款和条件中指出。应充分筛选所有应聘者、合同方和第三方用户，特别是对敏感岗位的成员。员工、合同方和信息处理设施的第三方用户要签署关于他们的安全角色和职责的协议。

有效的信息安全一定会关联到人员及其行为。应使各类人员在被任用前理解其在信息安全上的角色和职责，并通过任用前的筛查和任用合同的条款等手段以降低人员对信息安全的风险。

A.8.1.1 角色和职责

控制措施：应根据组织的信息安全方针，规定员工、合同方和第三方用户的安全角色和职责并形成文件。

内容解析：访问组织信息处理设施、接触或使用组织信息的全体人员都应承担信息安全责任。组织的信息安全方针通常只是简述信息安全的角色和职责，在人力资源管理或各单位的人员管理文件（例如，岗位职责说明）中应详细规定各类人员在信息安全方面负有的职责。

A.8.1.2 审查

控制措施：应根据相关的法律、法规和道德，对所有的求职者、合同方和第三方用户进行背景验证检查，该检查应与业务要求、接触信息的类别及已知风险相适宜。

内容解析：对所有待任用候选者（包括雇员、承包方人员和第三方人员）的背景都要进行审查，确保任用的职位和对组织的风险是相协调的。通常任用候选者对组织保密和敏感信息的访问范围越深对其审查力度越严。对背景的审查应与相关法规和具体的业务要求相一致。

A.8.1.3 任用条款和条件

控制措施：作为合同责任的一部分，员工、合同方和第三方用户应统一并签署他们的雇佣合同的条款和条件。这些条款和条件应规定他们和组织对于信息安全的责任。

内容解析：任用合同的条款和条件应清晰地说明进入到本组织所要承担的有关信息安全的职责。任用合同通常是较为复杂的法律文书，以保护组织的业务利益，包括组织对违反信息安全方针和要求而要采取的措施，有的条款甚至覆盖了离职后一段时间的责任。

A.8.2　任用中

目标：确保所有的员工、合同方和第三方用户了解信息安全威胁和相关事宜、他们的责任和义务，并在他们的日常工作中支持组织的信息安全方针，减少人为错误的风险。

内容解析：应确定管理职责来确保安全应用于组织内个人的整个雇用期。为尽可能减小安全风险，应对所有雇员、合同方和第三方用户提供安全程序和信息处理设施的正确使用方面的适当程度的意识、教育和培训。还应建立一个正式的处理安全违规的纪律处理。

使组织内部和外部的各方人员了解其工作环境关联的信息安全威胁、知晓对安全违规的处置，在业务运行中遵循安全方针、安全管理制度和规程，减少人为失误。

A.8.2.1　管理职责

控制措施：管理者应要求所有的员工、合同方和第三方用户按照组织已建立的方针和程序实施安全。

内容解析：管理层对制定、发布和监督执行信息安全方针策略、规程和指南以保护组织和员工的利益负有责任。为确保所有各方(内部或外部的)都能理解、遵守发布的方针策略、规程和指南，管理层应安排对安全方针策略的宣贯和执行状况进行监督；如果信息处理设施的用户未能清晰地意识到自身的信息安全职责，那么管理层也就不能确保安全方针策略得到遵循。

A.8.2.2　信息安全意识、教育和培训

控制措施：组织的所有员工，适当时，包括合同方和第三方用户，应受到与其工作职能相关的适当的意识培训和组织方针及程序的定期更新培训。

内容解析：组织信息处理设施的用户(包括雇员、承包方人员、合作方人员和第三方人员)都应接受针对其在组织内的角色和职能为具体目标的信息安全意识宣贯、教育或培训。培训意味着要培养新的概念并建立初步的基本技能；而教育则要提供相关的知识并进一步提升能力。

A.8.2.3　纪律处理过程

控制措施：应建立一个正式的员工违反安全的惩戒过程。

内容解析：针对违反信息安全方针策略和相关规定的员工，管理层要明确地规定、发布和执行纪律处理措施和过程。纪律处理过程应纳入信息安全意识的宣贯中以产生警示作用。

A.8.3　任用的终止或变化

目标：确保员工、合同方和第三方用户离开组织或雇佣变更时以一种有序的方式进行。

内容解析：应有合适的职责确保管理雇员、合同方和第三方用户从组织退出，并确保他们归还所有设备及删除他们的所有访问权力。组织内职责和工作的变化管理应符合本章内容，与职责或工作的终止管理相似，任何新的雇用应进行管理。

内部和外部各方人员的任用终止或任用状况的改变需要按书面的管理规定进行，避免信息安全的负面后果。

A.8.3.1 终止职责

控制措施：应清晰规定和分配进行雇佣中止或变更的责任。

内容解析：当一个员工或组织信息处理设施的外部用户被终止其职责或调动岗位时，管理层应有明确的过程确保工作的终止、交接或转换，充分考虑到对信息安全的保障。

A.8.3.2 资产的归还

控制措施：当雇佣、合同或协议终止时，员工、合同方和第三方用户应归还所使用的组织资产。

内容解析：所有的内部或是外部人员当其雇佣、协议或合同终止时都必须要求返还其所持有的全部组织资产(包括文件)。组织的管理文件或用人协议(或合同)的条款对此应有明确的规定；届时组织应指派专人接受并查验返还的资产。

A.8.3.3 撤销访问权

控制措施：当雇佣、合同或协议终止时，应撤销所有员工、合同方和第三方用户对信息和信息处理设施的访问权限，或根据变化调整。

内容解析：员工或外部相关人员一旦被终止职责或个人状况发生显著变化时应立即终止或消除其全部访问权，包括物理的和逻辑的。

5. A.9 物理和环境安全

A.9.1 安全区域

目标：防止对组织办公场所和信息的非授权物理访问、破坏和干扰关键或敏感的信息处理设施要放置在安全区域内，并受到一种已定义的安全边界的保护，包括适当的安全屏障和入口控制。这些设施要在物理上避免未授权访问、损坏和干扰。所提供的保护要与所标识的风险相匹配。

内容解析：组织周边内的场所应成为受控的安全区域，在物理和环境上要有保障措施，防止外界的干扰和擅自进入。

A.9.1.1 物理安全边界

控制措施：组织应使用安全边界(障碍物，如墙、卡控制的入口或人工接待台)来保护包含信息和信息处理设施的区域。

内容解析：组织信息处理设施的周边应通过物理控制措施给予充分的保护，物理控制措施包括围墙、栏杆、有人值守的入口、门禁和闭路电视等。至少信息处理系统和设施应置于一个人员进入受控的安全环境，最好使人员的进出受监视、有记录、可审计。

A.9.1.2 物理入口控制

控制措施：应通过适当的进入控制对安全区域进行保护，以确保只有经过授权的人员才可以访问。

内容解析：应对进入组织场所、工作区和安全区的入口设置物理控制(例如门禁)，以提供适当的保护。

A.9.1.3 办公室、房间和设施的安全保护

控制措施：应设计并实施保护办公室、房间和设施的物理安全防范外部或环境威胁，应设计并实施针对火灾、水灾、地震、爆炸、骚乱和其他形式的自然或人为灾难的物理保护措施。

内容解析：管理层应识别场所、办公室和组织设施的安全保护要求，并提供适当的物理控制保护。这些保护应是多方面的，不仅是人员或物品的进入控制，还包括视线、声音和电波的隔离屏蔽。

A.9.1.4 外部和环境威胁的安全防护

控制措施：为防止火灾、洪水、地震、爆炸、社会动荡和其他形式的自然或人为灾难引起的破坏，应设计和采取物理保护措施。

内容解析：为应对人为和自然灾害的威胁，组织应对其人员和重要资产提供充分而有效的物理保护。

A.9.1.5 在安全区域工作

控制措施：应设计并实施在安全区域工作的物理保护和指南。

内容解析：组织基于特定业务的保密要求（例如，关键技术开发）或其他安全考虑（有些考虑可能与信息安全无关，如人员安全、新设备的储存等）可在组织内设立安全区，将人员、设施环境以及相关的信息和工作产出物在组织内隔离。安全区通常应配备更强的物理控制、受到监视并具有审计能力。组织应制定并发布在安全区工作的要求。

A.9.1.6 公共访问、交接区安全

控制措施：访问区域如装卸区域及其他未经授权人员可能进入办公场所的地点应加以控制，如果可能，与信息处理设施加以隔离以防止非授权的访问。

内容解析：组织应明确划定作为接待来访、交付物品等的公共区域。公共区域应受到物理控制和监视。

A.9.2 设备安全

目标：防止资产的丢失、损坏或被盗，以及对组织业务活动的干扰应保护设备免受物理的和环境的威胁。

内容解析：对设备的保护（包括离开组织使用和财产移动）是减少未授权访问信息的风险和防止丢失或损坏所必需的。这样做还要考虑设备安置和处置。可能需要专门的控制用来防止物理威胁以及保护支持性设施，诸如电源供应和布缆基础设施。

对网络和计算机相关的设备需加以保护，防止环境上和物理上损坏，包括人为的破坏、盗窃及失误等行为。

A.9.2.1 设备安置和保护

控制措施：应对设备进行选址安置或保护，以减少来自环境的威胁或危害，并减少未授权访问的机会。

内容解析：这一控制措施的目的旨在保护网络和计算机设备免遭可能存在于组织内的环境和物理威胁。环境威胁包括温度、湿度、雷电等，物理威胁包括粉尘、振动、各类干扰和辐射等。

A.9.2.2 支持性设施

控制措施：应保护设备免受电力中断或其他因为支持性设施失效所导致的中断。

内容解析：支持性设施包括供电、供水、排污、通风、温/湿度调节设备等。这些设施的故障会对信息处理设施的正常运行产生影响。

组织应对支持性设施的运行和维护提供保障，避免电力中断和其他支持性设施的失效，以保护信息处理设施和业务运行。

A.9.2.3 电缆安全

控制措施：应保护承载数据或支持信息服务的电力和通信电缆免遭中断或破坏。

内容解析：网络和通信线缆应受到保护，避免受到自然和人为的损坏。通常网络和通信线缆在布线的设计和施工中都有相关的质量监管；但在组织日常的运营中针对临时拉线、无人照管的外部接线以及网络和通信端口的未经授权的使用应有相关的管理措施。

A.9.2.4 设备维护

控制措施：应正确维护设备，以确保其持续的可用性和完整性。

内容解析：信息处理设施中的关键系统和主机应按照制造商的指南加以维护确保对授权用户的可用性。

A.9.2.5 组织场所外的设备安全

控制措施：应对场外设备进行安全防护，考虑在组织边界之外工作的不同风险。

内容解析：组织应基于风险评估，对工作运行在组织场所外的设备采取安全保护措施。

A.9.2.6 设备的安全处置或再利用

控制措施：应检查包含存储介质的所有设备，以确保在销毁前所有敏感数据或授权软件已经被移除或安全重写。

内容解析：对含有储存介质的任何类型的计算装置和系统在对其处理或再利用前都应确保删除其中的敏感信息和注册软件。

A.9.2.7 资产的移动

控制措施：未经授权，不得将设备、信息或软件带离工作场所。

内容解析：未经授权的包含组织信息和数据的计算装置、软件或其他设备都不应带出组织的场所。

6. A.10 通信和操作管理

A.10.1 操作规程和职责

目标：确保信息处理设施的正确和安全操作。

内容解析：应建立所有信息处理设施的管理和操作职责和程序。这包括制定合适的操作程序。当合适时，应实施责任分离，以减少疏忽或故意误用系统的风险。

为安全地运行信息系统和处理设施，相关的操作规程、指南和方针策略对日常的运维工作尤为关键。此目标关注于信息处理设施的操作文件、变更管理、责任划分和运行环境。

A.10.1.1 文件化的操作规程

控制措施：应编制并保持文件化的操作程序，并确保所有需要的用户可以获得。

内容解析：管理层应针对信息系统和信息处理设施的用户制定并保持与信息安全相关的操作规程。基于组织的特征，这类操作规程的覆盖范围可能很广，如涉及个人数据备份、介质处理、邮箱的使用、机房的进入等。组织可结合风险评估以及信息安全方针、法律法规和组织的运营要求等因素制定这类管理规程或制度。

A.10.1.2 变更管理

控制措施：应控制信息处理设施及系统的变更。

内容解析：对受控环境内信息处理系统和设施的任何变更都可能影响业务的运行，并对信息安全产生影响。因此对信息处理设施的变更要严加控制和监督。通常对信息处理设

施和系统的变更需要经历规范的处理过程。

A. 10. 1. 3　责任分割

控制措施：应分离职责和区域，以降低未授权访问、无意识修改或滥用组织资产的机会。

内容解析：责任分割指将同一项工作任务或职能分配给不同的角色来承担以降低产生错误或不良行为的机会。例如，两个角色各自持有不同的钥匙才能打开门禁。有关信息安全的职责应加以适当的分割以降低对资产的未授权的、无意识的或恶意的操作和使用。

A. 10. 1. 4　开发、测试和运行设施分离

控制措施：应分离开发、测试和运营设施，以降低未授权访问或对操作系统变更的风险。

内容解析：开发、测试与运行环境的分离是为了保护业务运行环境内的设施及相关数据，降低对生产运行系统未授权修改的风险。测试与开发的分离是为了使测试能在模拟的生产环境中运行以验证交付的系统满足生产和使用的要求。

A. 10. 2　第三方服务交付管理

目标：实施并保持信息安全的适当水平，确保第三方交付的服务符合协议要求。

内容解析：组织应检查协议的实施，监视协议执行的一致性，并管理变更，以确保交付的服务满足与第三方商定的所有要求。

通常认为组织自身为第一方，组织服务的顾客为第二方，第三方则指独立于上述各方的个人或机构，包括合作伙伴、外部供应商、审核方等。组织为管理第三方交付的服务，应就服务的级别和信息安全要求形成协议，并据此监督服务交付行为和过程。

A. 10. 2. 1　服务交付

控制措施：确保第三方实施、运行并保持第三方服务交付协议中包含的安全控制、服务定义和交付等级。

内容解析：当组织需要第三方提供服务时，应与第三方签署服务交付协议，其中包括规定的服务、服务交付的级别和安全控制措施。组织应接受并查验第三方交付的服务，包括服务交付的行为、过程和结果，确保交付的服务满足协议的要求。

A. 10. 2. 2　第三方服务的监视和评审

控制措施：应对服务和第三方提交的报告定期进行监视和评审，并定期进行审核。

内容解析：由第三方提供的服务、产品或信息应定期进行监视和评审，证实履行协议中规定条款的准确性和符合性。监视第三方的服务交付需要配置一定的资源和技术能力，而评审服务应依据定期的服务报告和相关记录。

A. 10. 2. 3　第三方服务的变更管理

控制措施：应管理服务提供的变更(包括保持和改进现有信息安全方针、程序和控制措施)，考虑对业务系统的关键程度、涉及的过程和风险的再评估。

内容解析：第三方服务对某些组织是十分关键的。管理层必须考虑第三方服务的变更对组织业务以及对信息安全的影响。变更可以导致新的业务需求或增加功能，不论在哪种情况下都应评估变更对信息安全的风险并确保配合有适当的控制和保护措施。

A. 10. 3　系统规划和验收

目标：将系统失效的风险降至最小。

内容解析：为确保足够容量和资源的可用性以提供所需的系统性能，需要预先的规划和准备；宜做出对于未来容量需求的推测，以减少系统过载的风险；新系统的运行要求宜在验收和使用之前建立、形成文件并进行测试。

系统在规划时就要识别失效的风险，充分考虑信息安全和容量需求，确保系统的安全性并具有充分的能力；在系统验收时应通过正式的过程加以把控，保证所有的需求得到满足。

A.10.3.1 容量管理

控制措施：应监督、调整资源的使用情况，并反映将来容量的要求，以确保系统的性能。

内容解析：容量指信息处理系统或组件在一定运行性能时的最大吞吐量。对IT系统及不同的组件其容量的度量单位不同，如对网络用“带宽”，对CPU用“核数和频率”。容量对IT系统有时又称为能力。对支持关键业务的信息处理系统应监视其运行的性能级别和容量。通过监视和预测信息处理系统和组件的容量，制定容量管理计划来确保系统具有充分的容量满足业务目标。

A.10.3.2 系统验收

控制措施：应建立新的信息系统、系统升级和新版本的验收准则，并在开发过程中及接收前进行适当的系统测试。

内容解析：对新的系统或系统的升级验收，管理层应预先定义正式的测试准则。通常组织应制定并实施一个正式的验收过程。

A.10.4 防范恶意和移动代码

目标：保护软件和信息的完整性。

内容解析：要求有预防措施，以防范和检测恶意代码和未授权的移动代码的引入。

软件和信息处理设施对恶意代码(例如计算机病毒、网络蠕虫、特洛伊木马和逻辑炸弹)的引入是脆弱的。要让用户了解恶意代码的危险。若合适，管理者要引入控制，以防范、检测并删除恶意代码，并控制移动代码。

恶意代码是对信息处理系统的主要威胁之一，可产生很大的破坏力。移动代码在使用不当时也会产生与恶意代码相似的后果，从而威胁软件和信息的完整性。因此必须严格防范恶意代码，对移动代码也需要谨慎控制。

A.10.4.1 控制恶意代码

控制措施：应实施防范恶意代码的检测、预防和恢复，以及适当的用户意识程序。

内容解析：恶意代码是指恶意编制的一段程序，它通过删除或改写文件、发送电子邮件，使计算机和组件无法工作来攻击和破坏系统。恶意代码通常包括计算机病毒、蠕虫、特洛伊木马、逻辑炸弹、间谍软件和其他不良软件等。组织对恶意代码应备有检测、预防和恢复破坏等多种遏制手段，对不同的目标群采取相应的控制措施。

A.10.4.2 控制移动代码

控制措施：当使用移动代码获得授权时，配置管理应确保授权的移动代码按照明确定义的安全方针运行，并防止未经授权移动代码的执行。

内容解析：移动代码指可以从远程系统获得的软件模块，它通过网络传输下载到本地的系统，没有明显的安装和启动，激活后自动执行某种功能。恶意的移动代码意图破坏信息系统和计算机的性能或安全，增加对系统的访问，盗取未授权的信息，破坏信息、盗用系统资源或造成拒绝服务。

组织对信息处理系统和应用系统中的移动代码应特别关注，应开发和实施控制措施来检测未授权的移动代码防止其在信息处理系统和应用系统中运行。

A.10.5　备份

目标：保持信息和信息处理设施的完整性和可用性。

内容解析：应建立例行程序来执行商定的针对数据拷贝备份以及及时恢复演练的策略和战略。

为保持信息和信息处理设施的完整性及可用性，组织应建立并保持对数据信息、软件和相关文件进行备份的机制，对备份应进行定期测试。确保在发生诸如系统或存储介质故障等事件的情况下系统和信息能得以恢复。

A.10.5.1　信息备份

控制措施：应根据既定的备份策略对信息和软件进行备份并定期测试。

内容解析：组织的关键数据和信息包括业务应用数据、软件和系统配置应按照组织的备份策略定期备份，以便在紧急情况下用以恢复信息处理系统和业务或在需要的时候恢复原始信息。备份通常可分为日常备份和灾难备份。备份的信息应定期按恢复规程和业务联系性计划进行测试，确保能恢复数据和业务。

A.10.6　网络安全管理

目标：确保网络中的信息和支持性基础设施得到保护。

内容解析：可能跨越组织边界的网络安全管理，需要仔细考虑数据流、法律蕴涵、监视和保护。还可以要求附加的控制，以保护在公共网络上传递的敏感数据。

对组织内的网络应从网络管控及网络服务的角度来保证安全。对跨越组织边界的网络也需要考虑适当的控制措施，以保护在公共网络传递的数据。

A.10.6.1　网络控制

控制措施：应对网络进行充分的管理和控制，以防范威胁、保持使用网络的系统和应用程序的安全，包括信息传输。

内容解析：网络的管理和控制应结合适当的安全技术以实现预期的保护级别。为此首先应对全部网络活动明确管理职责，建立有关网络安全的管理规程和制度，指派专业人员或团队来管理和维护网络相关的设备、组件和服务，实施在线安全网络管理和网络安全监控。

A.10.6.2　网络服务安全

控制措施：应识别所有网络服务的安全特性、服务等级和管理要求，并包含在网络服务协议中，无论这种服务是由内部提供的还是外包的。

内容解析：网络服务包括提供接入、私有网络、增值网络、网络安全管理(含解决方案)等。为确保网络服务的安全，不论是采用内部单位还是外部第三方来提供服务，组织都应识别所需要的网络服务、服务的安全特性、服务级别以及对服务的管理要求，并在网络服务级别协议中做出明确规定。在协议中还应对网络服务方进行监管，以确保其具备约定的能力并满足相关要求。

A.10.7　介质处置

目标：防止对资产的未授权泄漏、修改，移动或损坏，及对业务活动的干扰应控制介质，并对其实施物理保护。

内容解析：为使文件、计算机介质(如磁带、磁盘)、输入/输出数据和系统文件免遭未授

权泄漏、修改、应建立适当的删除和销毁的操作程序。

介质是纸面的或电子化的、可移动的或相对固定的承载有信息的资产，这类资产在使用过程中如管理不当有可能造成信息的泄漏、修改、移动或销毁，甚至导致业务活动中断。对各类介质组织应有健全的管控措施。

A.10.7.1 可移动介质的管理

控制措施：应建立可移动介质的管理程序。

内容解析：可移动介质包括移动硬盘、USB盘、各种存储卡、CD-ROM、DVD盘、磁带和打印的纸张等。可移动介质(尤其是便携易传送电子介质)的使用对组织的信息安全带来风险，因而对员工使用可移动介质组织应按照定义的相关规程并在必要时结合技术措施加以适度的管理。

A.10.7.2 介质的处置

控制措施：当介质不再需要时，应按照正式的程序进行安全可靠的销毁。

内容解析：含有组织信息和数据的介质，当其不再需要保留或使用时，应按照组织发布的管理规程采用适当的方式加以销毁或处理(包括介质的再利用)。

A.10.7.3 信息处理规程

控制措施：应建立信息处置和存储程序，以防范该信息的未授权泄漏或误用。

内容解析：信息可以以书面或电子的方式记录和存储，通过人工或自动化的工具设施进行处理，并以多种方式进行通信。组织应基于信息的保密级别在信息的存储、处理和通信等各个环节上建立必要的安全操作规程，以防止对信息未授权的误用或毁坏。

A.10.7.4 系统文件安全

控制措施：应保护系统文档免受未授权的访问。

内容解析：为了将系统被侵入和损害的风险最小化，信息处理设施的系统文件应得到安全保护以防止未授权的访问。系统文件的范围可以很广泛，包括计算机系统文件、设备配置文件、网络拓扑图等。

A.10.8 信息的交换

目标：应保持组织内部或组织与外部组织之间交换信息和软件的安全。

内容解析：组织间信息和软件的交换应基于一个正式的交换策略，按照交换协议执行，还应服从任何相关法律。要建立程序和标准，以保护信息和在传输中包含信息的物理介质。

组织内以及与外部的相关方在业务活动中必然要进行信息沟通，组织内外间的信息交换应在管理制度、物理和逻辑上进行控制，以确保信息交换的安全。

A.10.8.1 信息交换策略和规程

控制措施：应建立正式的交换策略、程序和控制，以保护通过所有类型的通信设施交换信息的安全。

内容解析：为保障信息交换的安全，对组织内外的信息交换应制定和发布正式的策略和规程。由于存在范围广泛的信息交流和多种多样的信息交换方法，信息交换中的安全意识也是这项控制措施的要点。

A.10.8.2 交换协议

控制措施：应建立组织和外部组织信息和软件交换的协议。

内容解析：组织与外部相关方进行信息交换应建立法律协议，明确交换数据或信息的

类别、标记、管理职责、相关规程和技术标准等。交换协议可以是多种形式(例如,电子的或书面的)。这里的软件是指记录和阅读信息相关的软件。

A.10.8.3　运输中的物理介质

控制措施:在组织的物理边界之外进行传输的过程中,应保护包含信息的介质免受未授权的访问、误用或破坏。

内容解析:对于要传输的物理介质,不论采用何种传送方式(如快递、信使等)组织应都基于信息的保密级别对介质采取适当的保护措施。一旦含有保密信息的物理介质离开组织的边界,还应监视其在运输中的状态,直到安全接收。

A.10.8.4　电子消息发送

控制措施:应适当保护电子消息的信息。

内容解析:电子消息包括 EDI、E-mail、即时消息(如 QQ、MSN 等)、短消息或多媒体消息(如彩信),但不包含传真和通常的电话语音通信。对电子消息的保护主要在于防止未授权的截取、破坏或不正确的交付。

A.10.8.5　业务信息系统

控制措施:应开发并实施策略和程序,以保护与业务信息系统互联的信息。

内容解析:组织内不同业务或部门间的信息共享可通过信息系统和设施的互联,对关联信息共享系统的脆弱性和介入人员(包括不同类别的内部人员、承包方人员和业务伙伴人员)应加以识别控制,以保护与业务运营相关的共享信息(包括文件、视频、语音等),为此管理层应制定并实施相关的策略和规程。

A.10.9　电子商务服务

目标:确保电子商务的安全及它们的安全使用。

内容解析:应考虑与使用电子商务服务相关的安全蕴涵,包括在线交易和控制要求。还应考虑通过公开可用系统以电子方式公布的信息的完整性和可用性。

电子商务是一种高风险业务,从事电子商务的组织应提供安全的服务并确保服务使用的安全,包括提供完整准确的信息、保护客户的信息和确保交易安全。

A.10.9.1　电子商务

控制措施:应保护电子商务中通过公共网络传输的信息,以防止欺诈、合同争议、未授权的泄漏和修改。

内容解析:电子商务中的信息包括客户的信息(例如,注册信息、交易信息、订单等)和商家的业务信息。对电子商务通过公共网络传输的信息和数据应有保护措施,防止对信息的未授权的泄漏、修改和网络欺诈。

A.10.9.2　在线交易

控制措施:应保护在线交易中的信息,以防止不完整的传输、路由错误、未授权的消息修改、未经授权的泄漏、未经授权的消息复制或重放。

内容解析:电子商务的交易存在风险,消息可能被路由到错误的终端、消息被篡改或泄漏给未授权的人等。因此要采取适当的控制措施降低交易风险并满足相关法律法规的要求。

A.10.9.3　公共可用信息

控制措施:应保护公共可用系统中信息的完整性,以防止未经授权的修改。

内容解析：电子商务采用一种公共可用系统进行业务活动，其运营会处于较大的风险环境，因为接入因特网的任何一个人都可以访问，如果信息被篡改将可能面临各种纠纷。组织为保护信息应适时地开发、实施和评价控制措施，防止在公共可用系统中发布的信息遭受未授权的修改。

A.10.10 监视

目标：检测未经授权的信息处理活动。

内容解析：应监视系统，记录信息安全事件。应使用操作员日志和故障日志以确保识别出信息系统的问题。一个组织的监视和日志记录活动应遵守所有相关法律的要求。应使用系统监视检查所采用控制措施的有效性，并验证对访问策略模型的一致性。

监视信息处理设施中的关键系统和应用是一种高度有效的安全控制措施，组织应具备适当的监控手段以及管理机制，及时检测出信息处理环境中的未授权活动以便做出处置。

A.10.10.1 审计记录

控制措施：应产生记录用户活动、以外和信息安全事件的日志，并按照约定的期限进行保留，以支持将来的调查和访问控制监视。

内容解析：审计记录（或审计日志）是一种计算机文件，它记录了系统（尤其是应用系统）用户的全部活动，包括对记录的修改细节。审核记录可能包含敏感信息，例如用户的账户信息，应妥善加以保护，防止未授权的泄漏和破坏。

A.10.10.2 监视系统的使用

控制措施：应建立监视信息处理系统使用的程序，并定期评审监视活动的结果。

内容解析：对信息处理系统的基础设施和应用系统的正常运行及使用情况要加以监视。对监视结果应定期评审。对系统的监视包括运行监视（如针对系统的性能、占用的资源、带宽等）和安全监视（如入侵检测），对安全监视的人员必须要了解对系统和环境的威胁以识别潜在的危险。对监视系统的管理需要有相关的规程，确保监管人员能及时发现并处理问题，发挥监管资源的效能。

A.10.10.3 日志信息的保护

控制措施：应保护日志设施和日志信息免受破坏和未授权的访问。

内容解析：日志包括系统日志、审计日志和安全事态日志等。对记录日志的设施和日志信息应识别控制措施，妥善加以保护防止未授权的访问，确保信息的完整性。

A.10.10.4 管理员和操作员日志

控制措施：应记录系统管理员和系统操作者的活动。

内容解析：系统管理员和操作员对系统的操作行为应加以记录和监视。设定管理员级别的访问权可能有业务运行的要求，但如果被未授权的或含有不良意图的人所利用就会对系统和业务带来巨大风险。基于安全的考虑可在管理员控制范围之外实施某种入侵检测系统。

A.10.10.5 故障日志

控制措施：应记录并分析错误日志，并采取适当的措施。

内容解析：信息技术系统和应用有时会发生故障或错误。有的故障系统可自动告警和记录，有些故障则需要人工报告和记录。组织应对故障记录进行汇总，由维护人员进行分析并尽快处理。在这些故障中有些可能与安全有关，对可疑的活动需要继续跟踪监视并采取

适当的措施。

A.10.10.6 时钟同步

控制措施：组织内或同一安全域内的所有相关信息处理设施的时钟应按照约定的正确间隔保持同步。

内容解析：时钟同步在信息安全上是一个重要的因素，它确保安全日志记录了与其他网络组件和系统相关联的所有事态发生的准确时间，也是安全事件取证的依据。时间对安全事态也十分重要，因为它追踪了入侵者的路径。

7. A.11 访问控制

A.11.1 访问控制的业务要求

目标：控制信息访问。

内容解析：对信息、信息处理设施和业务过程的访问应在业务和安全要求的基础上予以控制。访问控制规则应考虑到信息传播和授权的策略。

A.11.1.1 访问控制策略

控制措施：应建立文件化的访问控制策略，并根据对访问的业务和安全要求进行评审。

内容解析：管理层应制定并发布一份访问控制策略文件，访问控制策略应满足组织对业务运行、法律法规、合同和其他特殊情况下的要求。访问控制是信息安全的关键概念，组织应十分关注访问控制的运行，并将当前实施状况与标准本条款的要求进行比较以改进访问安全。

A.11.2 用户访问管理

目标：确保授权用户的访问，并预防信息系统的非授权访问。

内容解析：应有正式的程序来控制对信息系统和服务的访问权力的分配。

这些程序应涵盖用户访问生存周期内的各个阶段，从新用户注册到不再要求访问信息系统和服务的用户的最终注销。在合适的情况下，应特别注意对有特权的访问权力的分配的控制需要，这种权力允许用户超越系统控制。组织信息处理设施的用户应按照访问控制策略并结合相应的方法加以鉴别和授权。

A.11.2.1 用户注册

控制措施：应建立正式的用户注册和解除注册程序，以允许和撤销对于所有信息系统和服务的访问。

内容解析：管理层应依据访问控制策略对需要访问信息处理系统和应用的用户实施注册和注销账户的规程。

A.11.2.2 特殊权限管理

控制措施：应限制和控制特权的使用和分配。

内容解析：特殊权限在信息安全中十分重要，因为特权是基于信任，通常只授予管理层和特定人员。特殊权限会给组织的资产带来安全风险，应按照规定策略和指南严格控制其分配和使用。在企业内控方面可以借鉴最小特权原则，即将访问权限制在履行其职责所需的最低限度。

A.11.2.3 用户口令管理

控制措施：应通过正式的管理流程控制口令的分配。

内容解析：口令是用来鉴别用户身份的一组秘密字符串，用来控制对数据、系统和网络的访问。口令管理是一个过程，包含对口令策略（规则）和管理规程的定义、实施和维护。有效的口令管理可降低对信息处理设施和信息的损害风险，保护口令的保密性、完整性和可用性。

A.11.2.4 用户访问权的复查

控制措施：管理者应按照策划的时间间隔通过正式的流程对用户的访问权限进行评审。

内容解析：对访问权应由不负责建立账户的有资质的人员进行定期的复查，以确保现有的访问权符合其角色和职责。

A.11.3 用户职责

目标：避免未授权用户的访问，信息和信息处理设施的破坏或被盗。

内容解析：已授权用户的合作是有效安全的基础。要让用户了解他对维护有效的访问控制的职责，特别是关于口令的使用和用户设备的安全的职责。应实施桌面清空和屏幕清空策略以减少未授权访问或破坏纸质文件、介质和信息处理设施的风险。

A.11.3.1 口令使用

控制措施：应要求用户在选择和使用口令时遵循良好的安全惯例。

内容解析：组织应基于良好的口令实践建立口令结构，用户要遵守组织的要求，并建立良好的口令使用习惯。

A.11.3.2 无人值守的用户设备

控制措施：用户应确保无人值守的设备得到适当的保护。

内容解析：当信息处理设施和应用系统处于无人值守时，管理层应有必要的措施确保无人值守的设备得到适当的保护。如当非工作时间，由值班人员对工作场所和设施进行定期巡查等。

A.11.3.3 清空桌面和屏幕策略

控制措施：应采用针对文件、可移动储存介质的桌面清空策略和针对信息处理设施的屏幕清空策略。

内容解析：当员工一段时间（如开会）不在工作区时，他们的工作区域应确保安全，任何形式的敏感信息未被非授权访问。对此组织应规定相应的策略或制度。

A.11.4 网络访问控制

目标：防止对网络服务未经授权的访问。

内容解析：对内部和外部网络服务的访问均应加以控制。访问网络和网络服务的用户不应损害网络服务的安全，应确保：

（1）在本组织的网络和其他组织拥有的网络或公共网络之间有合适的分界。

（2）对用户和设备有合适的认证机制。

（3）对用户访问信息服务的强制控制。

A.11.4.1 使用网络服务的策略

控制措施：用户应只能访问经过明确授权使用的服务。

内容解析：网络连接，特别是因特网和无线网连接，需要在信息处理环境中识别风险。管理层对使用网络服务以及日常监视网络环境应规定有明确的策略，以确保用户仅能访问得到授权的服务。

A.11.4.2　外部连接的用户鉴别

控制措施：应使用适当的鉴别方法控制远程用户的访问。

内容解析：应采用安全的鉴别方式来控制远程用户对信息处理设施的外部网络连接。常用的鉴别方法有：登录时要求用户名和口令。但对重要的系统组织应基于风险考虑其他鉴别方式，如生物鉴别等。

A.11.4.3　网络上的设备标识

控制措施：应考虑自动设备标识，将其作为鉴别特定位置和设备连接的方法。

内容解析：适当时，对网络上的设备进行标识，是鉴别来自一个特定受控环境和设备的网络通信的安全手段。

A.11.4.4　远程诊断和配置端口的保护

控制措施：应控制对诊断和配置端口的物理和逻辑访问。

内容解析：对网络和通信设备的诊断和远程端口，组织应严密控制，防止未授权的物理和逻辑访问。

A.11.4.5　网络隔离

控制措施：应隔离信息系统内的信息服务组、用户和信息系统。

内容解析：网络服务是基于网络的服务，包括因特网服务、内部网络、无线网络、IP 电话和视频广播等。在可能的情况下应将网络服务在逻辑网络中进行隔离，以增强控制的深度。

A.11.4.6　网络连接控制

控制措施：在公共网络中，尤其是那些延展到组织边界之外的网络，应限制用户连接的能力，并与业务应用系统的访问控制策略和要求一致。

内容解析：网络扩展到组织的边界之外通常是为了便利与外部第三方供应商或外部商业合作伙伴开展业务活动。从信息安全的角度，对这种网络连接控制是一种挑战，而且常被忽略，因为供应商和业务伙伴在使用组织网络时是受信的。所以组织应实施控制措施来限制用户的连接能力和对网络的访问能力。

A.11.4.7　网络路由控制

控制措施：应对网络进行路由控制，以确保信息连接和信息流不违反业务应用系统的访问控制策略。

内容解析：网络路由的逻辑控制对数据和信息流的控制十分关键。网络路由的控制应与对特定应用和服务的访问控制相结合。网络路由控制通常需要在 IT 部门选择具有相关知识的人员来设计和实施本项所要求的控制措施，并最好经过相关专家的确认。

A.11.5　操作系统访问控制

目标：防止对操作系统的未授权访问。

内容解析：安全设施应该用来限制授权用户访问操作系统。这些设施应该包括下列内容：

(1) 按照已定义的访问控制策略鉴别授权用户。

(2) 记录成功和失败的系统认证尝试。

(3) 记录专用系统特权的使用。

(4) 当违背系统安全策略时发布警报。

(5) 提供合适的认证手段。

(6) 恰当处可限制用户的连接次数。

A.11.5.1 安全登录规程

控制措施：应通过安全登录程序对操作系统的访问进行控制。

内容解析：操作系统的访问应通过安全设计的登录和鉴别规程来加以保护，将未授权访问的机会降低到最小。

A.11.5.2 用户标识和鉴别

控制措施：所有的用户应有一个唯一的识别码(用户 ID)且仅供本人使用，应使用适当的鉴别技术来证实用户所声称的身份。

内容解析：对组织信息处理系统访问的用户应有唯一的用户账户，并在允许其访问系统前采用安全的方式来确认用户的身份。

A.11.5.3 口令管理系统

控制措施：应使用交互式口令管理系统，并确保口令质量。

内容解析：应采用系统来管理口令并强制实施口令策略。口令管理系统通常与网络相关联，但也可应用于应用系统和数据库。

A.11.5.4 系统实用工具的使用

控制措施：应限制并严格控制设施程序的使用和应用系统控制的使用。

内容解析：对于超越系统控制的实用工具应限制安装，如需安装使用，其使用权限应仅限于指定的管理员。对实用工具的使用应加以监视并保留记录。

A.11.5.5 会话超时

控制措施：不活动的会话应在一个设定的不活动周期后关闭。

内容解析：操作系统和终端在预定的时间段内，如会话没有活动应自动加锁，以防止未授权访问。

A.11.5.6 联机时间的限定

控制措施：应使用连接时间限制以提供高风险应用程序的额外安全保障。

内容解析：对识别为高风险的应用系统，在联机时间上要有限制，超过约定联机时间应加锁或断开联机。

A.11.6 应用和信息访问控制

目标：防止对应用系统中信息的未授权访问，安全设施应该将访问限制在应用系统之内。

内容解析：对应用软件和信息的逻辑访问只限于已授权的用户。应用系统应：

(1) 按照定义的访问控制策略，控制用户访问信息和应用系统功能。

(2) 防止能够越过系统控制或应用控制的任何实用程序、操作系统软件和恶意软件进行未授权访问。

(3) 不损坏共享信息资源的其他系统的安全。

A.11.6.1 信息访问限制

控制措施：应根据规定的访问控制策略，限制用户和支持人员对信息和应用系统功能的访问。

内容解析：应用系统具有储存和处理关键、敏感信息和数据的能力。组织对这类数据和信息应依照已确定的访问控制策略采取保护性的控制措施(例如，限制访问权限，包括读、

写、删除等),以防止未授权的访问及信息损毁。

A.11.6.2　敏感系统隔离

控制措施:敏感系统应使用独立的计算环境。

内容解析:如果识别为高敏感性的应用系统,应加以隔离、严密控制并监视。同时对信息处理系统或应用系统的责任人,也应有相应的隔离要求。

A.11.7　移动计算和远程工作

目标:确保在使用移动计算和远程工作设施时信息的安全。

内容解析:所要求的保护应与那些特定工作方法引起的风险相匹配。当使用移动计算时,应考虑不受保护的环境中的工作风险,并且要应用合适的保护。在远程工作的情况下,组织要把保护应用于远程工作场地,并且对这种工作方法,确保合适的安排到位。

A.11.7.1　移动计算和通信

控制措施:应建立正式的策略并实施适当的控制,以防范使用移动计算和通信设施的风险。

内容解析:移动计算是指可改变位置的计算装置,通常包括便携式计算机、PDA、超级移动计算机、智能手机、车载计算机。移动计算的使用,因为处在受控的网络环境之外,所以是组织面临的特殊风险,需要组织策划相应的控制措施。

A.11.7.2　远程工作

控制措施:应开发并实施远程工作的策略、操作计划和程序。

内容解析:远程工作是指利用信息通信技术(ICT)使工作能在远离工作结果产生的地点进行,例如,居家远程工作。远程工作者需要访问组织的资源,包括内部应用系统和信息。所以组织应明确远程工作策略,并针对从外部访问组织资源的相关风险,开发和实施特定的控制和防护措施。

8. A.12　信息系统获取、开发和维护

A.12.1　信息系统的安全要求

目标:确保安全成为信息系统的有机组成部分。

内容解析:这将包括操作系统、基础设施、业务应用、非定制的产品、服务和用户开发的应用。支持应用或服务的业务过程的设计和实施可能是安全的关键。在信息系统开发之前应商定并标识出安全要求。

应在项目的要求阶段标识出所有安全要求,并证明这些安全要求是正确的,对这些安全要求加以商定,并且将这些安全要求形成文档作为信息系统整个业务情况的一部分。

A.12.1.1　安全要求分析和说明

控制措施:新的信息系统或对现有信息系统的更新的业务要求声明中应规定安全控制的要求。

内容解析:在建设一个新的信息系统前或是对现有系统进行升级时,必须要识别和定义信息安全的需求和控制措施。信息安全的要求和控制措施进入设计过程最为有效,决不能放在以后再说。

A.12.2　应用中的正确处理

目标:防止应用系统信息的错误、丢失、未授权的修改或误用。

内容解析：应用系统（包括用户开发的应用）内应设计合适的控制以确保处理的正确性。这些控制应包括输入数据、内部处理和输入数据的确认。

对于处理敏感的、有价值的或关键的组织资产的系统或对上述组织资产有影响的系统可以要求附加控制。这样的控制应在安全要求和风险评估的基础上加以确定。

A.12.2.1 输入数据确认

控制措施：应验证应用系统输入数据，以确保正确和适当。

内容解析：数据和信息是业务应用系统的核心和灵魂。对输入信息处理系统或应用系统中的数据应确认其正确性（包括数据的边界、长度和业务逻辑等），并对系统可接受的输入类型进行确认检查以保证数据是恰当的，避免不符合要求的数据进入系统。在软件开发中通常都会对输入数据进行确认，但对通过自动捕获得到的数据和信息却容易忽略。所以在对输入数据进行确认时，需同时需要关注自动捕获的数据和信息。

A.12.2.2 内部处理的控制

控制措施：应用系统中应包含确认检查，以检测数据处理过程中的错误。

内容解析：正确输入的数据可能会因硬件错误、处理出错或故意的行为而破坏。应用系统应在数据的处理过程设置错误检查，必要时提供数据变更、中断处理及恢复功能。

A.12.2.3 消息完整性

控制措施：应识别应用系统中确保鉴别和保护消息完整性的要求，识别并实施适当的控制。

内容解析：许多应用系统使用内部消息进行运行和处理。这些应用消息应加以保护以确保对数据不发生未授权的修改或损坏。

A.12.2.4 输出数据确认

控制措施：应确认应用系统输出的数据，以确保存储的信息的处理是正确的并与环境相适宜。

内容解析：对关键应用系统的输出应进行确认，以确保输出数据是准确适当的。

A.12.3 密码控制

目标：通过加密手段来保护信息的保密性、真实性或完整性。

内容解析：应该制定使用密码的策略。密钥管理应该支持使用密码技术。

A.12.3.1 使用密码控制的策略

控制措施：为保护信息，应开发并实施加密控制的使用策略。

内容解析：密码控制是保护信息和数据防止未授权的访问或破坏的防护措施。尽管其对保护信息和数据的保密性和完整性十分有效，但组织还应基于风险评估来拟定其使用范围。在组织管理方面应制定和发布使用密码的策略。

A.12.3.2 密钥管理

控制措施：应进行密钥管理，以支持组织对密码技术的使用。

内容解析：对于使用密钥的组织应具备一个正式的密钥管理系统来保护密钥，防止密钥被盗、误用和修改。

A.12.4 系统文件的安全

目标：确保系统文件的安全。

内容解析：要严格控制访问系统文件和程序源代码。按安全方式管理 IT 项目和支持

活动。在测试环境中应注意不能泄漏敏感数据。

A.12.4.1 运行软件的控制

控制措施:应建立程序,对操作系统软件安装进行控制。

内容解析:确保只有经过授权的软件、应用程序或系统才能安装在运行的信息处理系统中。

A.12.4.2 系统测试数据的保护

控制措施:应谨慎选择测试数据,并加以保护和控制。

内容解析:系统测试是对系统投入运行前或变更后的验证和确认,应谨慎设计和选择测试用例和数据,其中不应包含敏感信息(如个人的信息,业务数据等)。系统测试数据也是一种历史资源,有助于系统的运行维护人员对系统的故障和安全事态快速应对。所以测试数据应加以妥善保护和控制。

A.12.4.3 对程序源代码的访问控制

控制措施:应限制对程序源代码的访问。

内容解析:源代码是软件程序和应用系统的核心机密,在开发过程中应通过配置管理(及工具)实施严格的配置控制;软件产品或应用系统进入生产环境后还应纳入最终软件库;通过软件开发和运行中的访问控制和变更控制防止对源代码的未授权的访问、修改或损毁。

A.12.5 开发和支持过程中的安全

目标:保持应用系统软件和信息的安全。

内容解析:应严格控制项目和支持环境。负责应用系统的管理者,也应负责项目和支持环境的安全。他们应确保评审所有建议的系统变更,以检验这些变更既不损坏该系统也不损害操作环境的安全。

A.12.5.1 变更控制规程

控制措施:应通过正式的变更控制程序,控制变更的实施。

内容解析:对系统、应用、数据和网络装置的变更应通过正式的变更控制过程加以严格控制。

A.12.5.2 操作系统变更后应用的技术评审

控制措施:当操作系统变更后,应评审并测试关键的业务应用系统,以确保变更不会对组织的运营或安全产生负面影响。

内容解析:在核心运行系统发生变更后,组织应就其对一些关键应用系统的影响,组织正式的技术评审,识别对信息安全和业务产生的其他负面影响,以便采取措施尽快消除问题。

A.12.5.3 软件包变更的限制

控制措施:不鼓励对软件包进行变更。对必要的更改严格控制。

内容解析:无论是通过购买还是组织内自主研发的应用软件,都应尽可能避免修改以有助于控制那些未识别的或未预期的安全漏洞。对必要的变更组织应做好策划和组织,最好将多项变更组合在一起,一次实施,以降低变更带来的风险。

A.12.5.4 信息泄漏

控制措施:防止信息泄漏的可能性。

内容解析：通过介质、应用、系统和其他渠道泄漏的敏感信息，会对组织造成严重的负面影响。信息泄漏的方式较多，例如，在逻辑方面包括网络连接、存储介质；在物理方面包括纸片或文件；人员方面包括员工失误、恶意行为等，需要组织谨慎设计和实施多种控制措施防止信息泄漏。

A.12.5.5　外包软件开发

控制措施：组织应对软件外包开发进行监控。

内容解析：确定将应用软件系统开发部分或全部发包给外部机构时，需要拟定对承包方的管理和控制措施。

A.12.6　技术脆弱性管理

目标：减少由利用公开的技术脆弱点带来的风险。

内容解析：技术脆弱点管理应该以一种有效的、系统的、可反复的方式连同可确保其有效性的措施来实施。这些考虑应包括用操作系统和任何其他的应用。

A.12.6.1　技术脆弱性的控制

控制措施：应及时获得组织所使用的信息系统的技术脆弱点的信息，评估组织对此类技术脆弱点的保护，并采取适当的措施。

内容解析：组织应通过对系统和应用软件制造商有关安全脆弱性公告的监视或与有关的权威检测机构确立脆弱性通告机制来及时获取新的技术脆弱性信息，并针对发布的这类信息审查组织的系统、评价暴露程度并采取适当的处理措施（如安装补丁）。

9. A.13　信息安全事件管理

A.13.1　报告信息安全事态和弱点

目标：确保与信息系统有关的信息安全事态和弱点能够以某种方式传达，以便及时采取纠正措施。

内容解析：宜有正式的事态报告和上报规程。所有雇员、承包方人员都宜了解这些规程，以便报告可能对组织的资产安全造成影响的不同类型的事态和弱点。宜要求他们尽可能快地将信息安全事态和弱点报告给指定的联系点。

A.13.1.1　报告信息安全事态

控制措施：信息安全事态应尽可能快地通过适当的管理渠道进行报告。

内容解析：信息安全事态是已识别的或受怀疑但尚未确认的安全事件。对信息安全事态的报告，组织应规定适当的报告渠道；依组织规模和结构，可统一渠道或分层级报告。

报告安全事态是启动整个信息安全事件处理过程的触发点，应使所有的员工或用户都能清楚地了解安全事件的报告渠道和过程，以便一旦发现安全事态，尽快报告。

A.13.1.2　报告安全弱点

控制措施：应要求信息系统和服务的所有雇员、承包方人员和第三方人员记录并报告他们观察到的或怀疑的任何系统或服务的安全弱点。

内容解析：所有受怀疑的或识别的安全弱点都应该按规定的过程报告给管理层。在执行控制措施过程中需要两个维度。

（1）建立环境和过程使得信息系统的用户对观察到的安全弱点或威胁上报管理层。

（2）意识和培训，持续警醒用户可能身处的各类弱点和威胁。

A.13.2　信息安全事件和改进的管理

目标：确保采用一致和有效的方法对信息安全事件进行管理。

内容解析：宜有职责和规程，以便一旦信息安全事态和弱点报告上来，就能有效地处理它们，宜使用一个连续的改进过程对信息安全事件进行响应、监视、评价和整体管理。如果需要证据，则宜收集证据以确保符合法律要求。

A.13.2.1　职责和规程

控制措施：应建立关联职责和规程，以确保快速、有效和有序地响应信息安全事件。

内容解析：信息安全事件可能对相关各方产生压力甚至恐慌。组织应预先制定处理信息安全事件的管理职责、过程及相关的规程。确保在发生安全事件，尤其是在信息系统遭到攻击时能及时有效地做出响应。

A.13.2.2　对信息安全事件的总结

控制措施：应有一套机制量化和监视信息安全事件的类型、数量和代价。

内容解析：管理层应采用某种方法或系统，确保能采集到安全事件处理过程中的适当信息，以便在事后做出分析总结，吸取教训和评价改进。

对信息安全事件的总结可作为安全事件处理过程的一部分，也可形成单独的规程。通常在重大事件后要求提交正式的报告，分析事件原因和模式，量化直接和间接成本或损失，建议后续的行动方案等；评审现有相关的策略和控制措施，包括实施范围和适用性，提出改进建议。

A.13.2.3　证据的收集

控制措施：当一个信息安全事件涉及诉讼（民事的或刑事的），需要进一步对个人或组织进行起诉时，应收集、保留和呈递证据，以使其符合相关管辖区域对证据的要求。

内容解析：在很多情况下，信息安全事件会产生法律牵连。在信息安全事件处理过程中需要采集和保留相关的证据。组织对此应制定规程和指南。

10. A.14　业务连续性管理

A.14.1　业务连续性管理的信息安全方面

目标：防止业务活动中断，保护关键业务过程免受信息系统重大失误或灾难的影响，并确保它们的及时恢复。

内容解析：为提高使用预防和恢复措施，将对组织的影响减少到最低，并从信息资产的损失中恢复到可接受的程度，宜实施业务连续性管理过程。这个过程宜确定关键的业务过程，并宜将业务连续性的信息安全管理要求同其他的连续性一起如运行、员工、材料、运输和设施等结合起来。

A.14.1.1　在业务连续性管理过程中包含信息安全

控制措施：应为贯穿于组织的业务连续性开发和保持一个管理过程，以解决组织的业务连续性所需的信息安全要求。

内容解析：为了保持组织在重大事件和灾害后的业务运行能力，组织应制定和保持一个业务连续性管理过程，其中包括业务连续性计划或恢复计划。当业务运行中断时，按照业务连续性计划恢复的运行环境应能在某种程度上保持对原生产环境的保护和恢复。组织应基于风险评估确立在业务系统恢复过程中以及在恢复的系统运行中对信息安全的要求，以

便将所需的资源和措施纳入计划。

A.14.1.2 业务连续性和风险评估

控制措施：应识别能引起业务过程中断的事态，连同这种中断发生的概率和影响，以及它们对信息安全所造成的后果。

内容解析：风险评估是业务连续性管理的关键要素之一。对业务连续性进行风险评估时，需关联与信息安全相关的风险，如重大信息安全事件的发生及其后果等，作为策划业务连续性计划或恢复计划的输入。

A.14.1.3 制定和实施包含信息安全的连续性计划

控制措施：应制定和实施计划来保持或恢复运行，以在关键业务过程中断或失败后能够在要求的水平和时间内确保信息的可用性。

内容解析：组织在制定业务连续性计划时应基于对信息安全的要求、安全风险及其后果，并将相关的控制措施融入计划。在业务连续性计划的落实活动中应评估所实施的安全控制措施是否能确保恢复的系统、应用和环境的安全运营。

A.14.1.4 业务连续性计划框架

控制措施：应保持一个唯一的业务连续性计划框架，以确保所有计划是一致的，能够协调地解决信息安全要求，并为测试和维护确定优先级。

内容解析：基于组织关键业务的规模和范围，业务连续性计划可以是一个综合性的计划，包括多项业务、多个领域的恢复职责和工作计划（如场所设施、系统环境、数据和业务运行恢复等）。组织应保持统一的业务连续性计划架构，确保信息安全的要求和控制措施能在各项计划的实施过程中保持协调。

A.14.1.5 测试、维护和再评估业务连续性计划

控制措施：业务连续性计划应定期测试和更新，以确保其及时性和有效性。

内容解析：为了确保在发生业务中断时，信息处理环境和业务能有序地恢复，组织应定期对计划进行演练和评审，以测试计划的有效性，培训人员意识，发现实施能力和计划的不足，以便相应地做出改进。

11. A.15 符合性

A.15.1 符合法律要求

目标：避免违反法律、法规、规章、合同要求和其他的安全要求。

内容解析：信息系统的设计、运行、使用和管理都要受法律法规要求的限制，以及合同安全要求的限制。

特定的法律要求方面的建议应从组织的法律顾问或者合格的法律从业人员处获得。法律要求因国家而异，而且对于在一个国家所产生的信息发送到另一国家（即越境的数据流）的法律要求也不同。

A.15.1.1 可用法律的识别

控制措施：对每一个信息系统和组织而言，所有相关的法律、法规和合同要求，以及为满足这些要求组织所采用的方法，应加以明白地定义、形成文件并保持更新。

内容解析：识别与信息安全相关的全部法律法规和合同的要求是执行管理层的职责，组织应将为满足这些要求而采用的策略、方法、措施和相关人员的职责形成文件。

A.15.1.2　知识产权(IPR)

控制措施:应实施适当的程序,以确保在使用与知识产权有关的材料和软件时符合法律法规和合同要求。

内容解析:知识产权是指对智力劳动成果依法所享有的占有、使用、处置和收益的权利。组织应制定有关规程,确保对涉及知识产权的事项符合法律、法规和合同的要求。

A.15.1.3　保护组织的记录

控制措施:应按照法律法规、合同和业务要求,保护重要记录免受损失、破坏或伪造篡改。

内容解析:组织的业务和管理活动产生的大量记录,其中可能包含敏感信息。组织应按照法律法规、合同以及业务要求制定并实施有关记录管理的规定和规程,以保护组织的记录,防止未授权的访问、修改、损坏和销毁。

A.15.1.4　数据保护和个人信息的隐私

控制措施:应确保按适用的法律法规、合同条款的要求来保护数据和隐私。

内容解析:组织应按照法律法规的要求保护员工和顾客的个人信息。通常应制定并实施保护数据和个人信息隐私策略,并由指定的责任人负责处理相关事宜。

A.15.1.5　防止滥用信息处理设施

控制措施:应禁止用户把信息处理设施用于非授权的目的。

内容解析:组织建立的信息处理设施的目的是为了进行业务以及业务相关活动的。组织应规定哪种非业务需要而使用信息处理设施的行为是不恰当或滥用(例如,未经授权试图进入非授权访问的系统,在上班时间炒股或玩网络游戏等),并告知用户对使用信息处理设施的行为是否有监视手段。组织使用的监视工具或监视记录应符合相关法律法规的要求。

A.15.1.6　密码控制措施的规则

控制措施:使用密码控制时,应确保遵守相关的协议、法律法规。

内容解析:密码控制措施的使用是为了保护组织资产的保密性和完整性,但首先要了解国际上和我国有关密码控制的法律法规要求(例如,对执行密码功能的计算机软硬件的进出口限制,以及使用密码的限制)。在涉及密码控制领域开展业务活动和安全管理时确保符合法律法规的限制要求。为此组织应制定有关使用密码控制措施的文件,对密码控制措施的使用提供指南。

A.15.2　符合安全策略和标准以及技术符合性

目标:确保系统符合组织安全方针和标准。

内容解析:应定期评审信息系统的安全。

这种评审应根据相应的安全策略和技术平台进行,而对信息系统也应进行审核,看其是否符合安全实施标准和文档安全控制。

A.15.2.1　符合安全策略和标准

控制措施:管理者应确保在其职责范围内的所有安全程序得到了正确实施,以符合安全方针和目标。

内容解析:管理层为确保组织发布的各项安全方针策略和标准得到普遍的遵循,应有适当的检查或审核手段,组织的各级管理者对其职责范围内安全管理除了日常关注还应定期进行评审。

A.15.2.2　技术符合性核查

控制措施：应定期检查信息系统与安全实施标准的符合程度。

内容解析：为确保敏感信息和信息处理设施的安全，组织会采取各种措施，其中包括技术方法和手段在内的技术措施。这些技术措施是否达到了预定的安全标准和要求，组织需在安全技术人员（包括外部专家或第三方机构）的参与下对信息系统进行定期的核查，以验证技术安全保护和控制措施持续有效、满足要求。对系统进行必要的测试（如渗透测试）和评估（如脆弱性评估）。核查结果形成报告并提交管理层。

A.15.3　信息系统审计考虑

目标：最大化信息系统审计的有效性，最小化来自/对信息系统审计的影响。

内容解析：为保护审计工具的完整性和防止滥用审计工具，也要求有保护措施。

A.15.3.1　信息系统审计控制措施

控制措施：应谨慎策划对操作系统检查所涉及的审计要求和活动并获得许可，以最小化对业务过程的影响或风险。

内容解析：对信息系统可进行内部或外部审计，外部审计通常是为满足特定要求而进行的。组织的相关人员应与审计方进行仔细的策划和协调，使审计过程尽量避免或减少对组织业务运行的影响，并满足审计目标和要求。

A.15.3.2　信息系统审计工具的保护

控制措施：应限制对信息系统审计工具的访问，以防止可能的误用或损坏。

内容解析：审计工具具有揭示受保护信息和隐私信息的能力。组织对此应特别小心，防止审计工具受到未授权的安装、使用或是被滥用。

思考题

1. 影响选择控制措施的因素和条件有哪些？
2. 叙述选择控制措施的过程。
3. 详细解释风险管理方法。
4. 试述控制措施“信息安全的管理承诺”中管理者应考虑的内容。
5. 试述控制措施“保密性协议”中需考虑的因素。
6. 查阅资料、归纳第三方服务交付管理的控制目标、控制措施及实施要素。

第10章 信息系统安全等级保护标准体系

10.1 信息系统安全等级保护

10.1.1 等级保护概述

1994 年,国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定计算机信息系统实行信息系统安全等级保护。1999 年,颁布 GB 17859—1999《计算机信息系统安全保护等级划分准则》。2003 年,中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号)中明确指出:“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统,抓紧建立信息系统安全等级保护制度,制定信息系统安全等级保护的管理办法和技术指南。”2004 年,公安部等四部委《关于信息系统安全等级保护工作的实施意见》(公通字[2004]66 号)也指出:“信息系统安全等级保护制度是国家在国民经济和社会信息化的发展过程中,提高信息安全保障能力和水平,维护国家安全、社会稳定和公共利益,保障和促进信息化建设健康发展的一项基本制度。”之后我国又相继颁布了《电子政务信息安全等级保护实施指南(试行)》(国信办[2005]25 号)、《信息系统安全保护等级定级指南》、《信息安全等级保护管理办法(试行)》(公通字[2006]7 号)和《信息安全等级保护管理办法》(公通字[2007]43 号)等支撑信息安全等级保护实施的规范和标准。2008 年,颁布 GB/T 22239—2008《信息安全技术信息系统安全等级保护基本要求》和 GB/T 22240—2008《信息安全技术信息系统安全等级保护定级指南》。

1. 等级保护的含义

信息安全等级保护是指根据信息系统在国家安全、经济安全、社会稳定和保护公共利益等方面的重要程度,结合系统面临的风险、应对风险的安全保护要求和成本开销等因素,将其划分成不同的安全保护等级,采取相应的安全保护措施,以保障信息和信息系统的安全。

2. 等级保护的原则

(1) 重点保护原则:等级保护要突出重点,重点保护关系国家安全、经济命脉、社会稳定等方面的重要信息系统,集中资源首先确保重点系统安全。

(2)“谁主管谁负责、谁运营谁负责”原则：等级保护要贯彻“谁主管谁负责、谁运营谁负责”的原则，由各主管部门和运营单位依照国家相关法规和标准，自主确定信息系统的安全等级并按照相关要求组织实施安全防护。

(3) 分区域保护原则：等级保护要根据各地区、各行业信息系统的重要程度、业务特点和不同发展水平，分类、分级、分阶段进行实施，通过划分不同安全保护等级的区域，实现不同强度的安全保护。

(4)“同步建设、动态调整”原则：信息系统在新建、改建、扩建时应当同步建设信息安全设施，确保信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其他原因，安全保护等级需要变更的，应当重新确定系统的安全保护等级。

3. 信息系统安全保护等级划分

(1) 第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

(2) 第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

(3) 第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

(4) 第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

(5) 第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

4. 不同等级的安全保护能力

(1) 第一级安全保护能力：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

(2) 第二级安全保护能力：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

(3) 第三级安全保护能力：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

(4) 第四级安全保护能力：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难，以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

(5) 第五级安全保护能力：(略)。

10.1.2　等级保护实施方法与过程

1. 等级保护实施方法

实行信息系统安全等级保护时，要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理。信息系统安全等级保护的实施方法如图 10-1 所示。

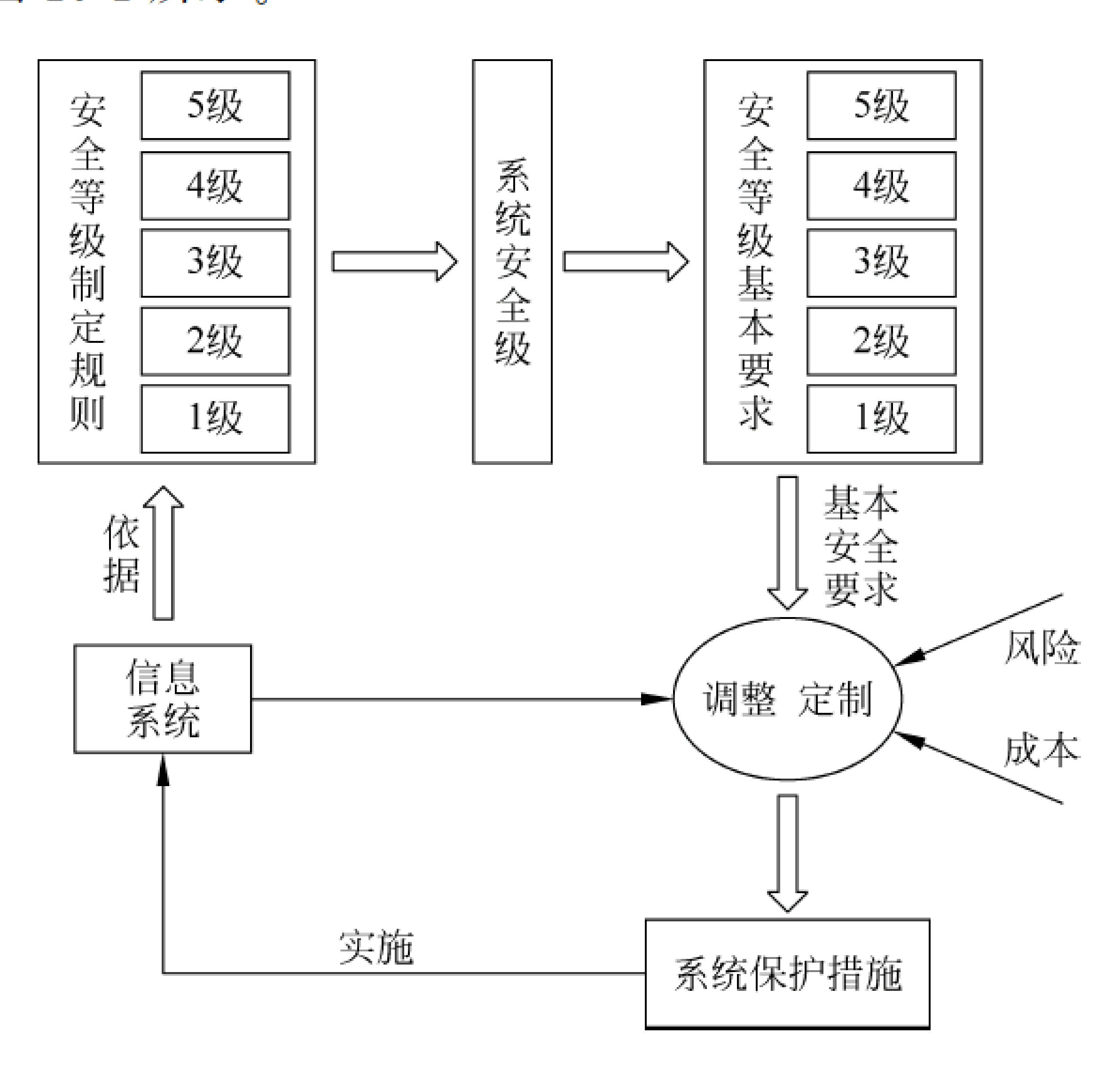


图 10-1　信息系统安全等级保护的实施方法

信息系统安全等级保护的实施方法中主要涉及以下内容。

(1) 安全定级：对系统进行安全等级的确定。

(2) 基本安全要求分析：对应安全等级划分标准，分析、检查系统的基本安全要求。

(3) 系统特定安全要求分析：根据系统的重要性、涉密程度及具体应用情况，分析系统特定安全要求。

(4) 风险评估：分析和评估系统所面临的安全风险。

(5) 改进和选择安全措施：根据系统安全级别的保护要求和风险分析的结果，改进现有安全保护措施，选择新的安全保护措施。

(6) 实施：实施安全保护。

2. 等级保护实施过程

图 10-2 给出了实施信息系统安全等级保护的总体流程，包括三个阶段，分别如下：

(1) 定级阶段。

(2) 规划与设计阶段。

(3) 实施、等级评估与改进阶段。

等级保护的基本流程如图 10-3 所示。

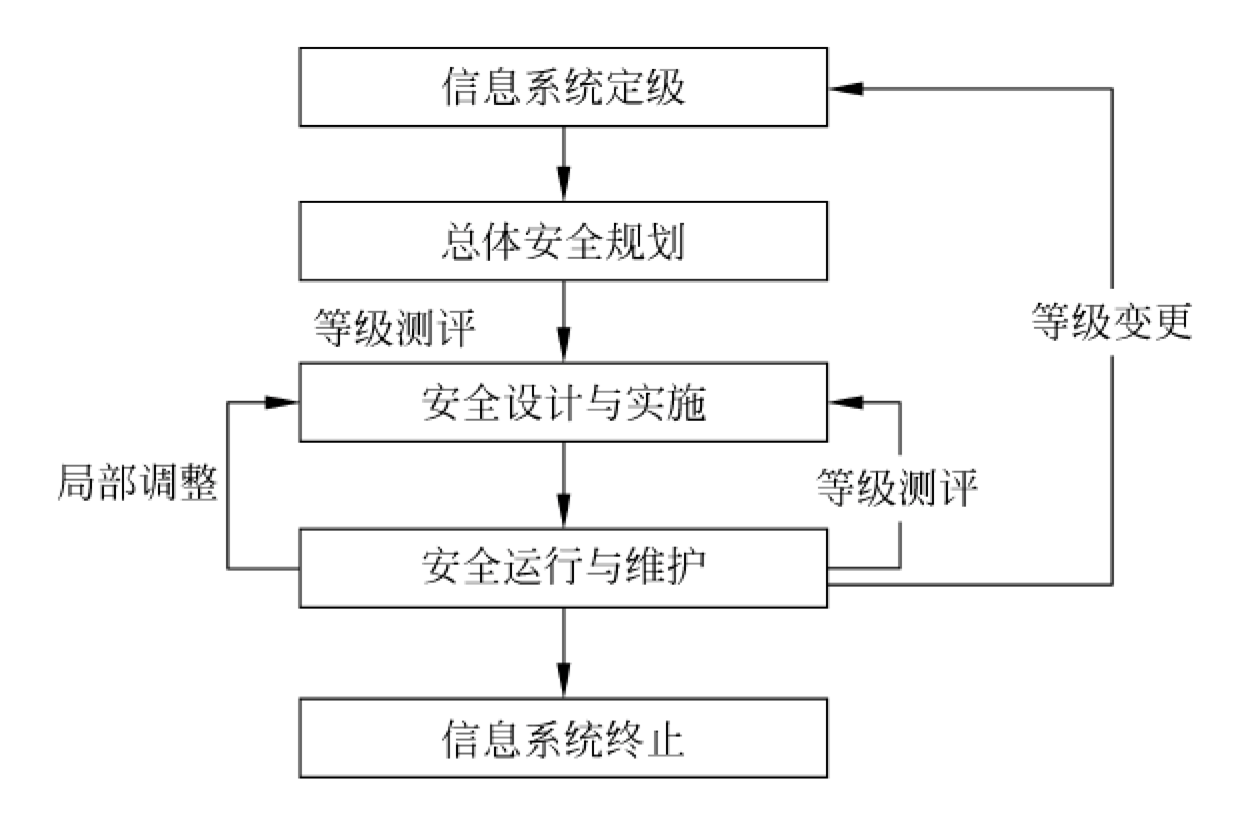


图 10-2　信息系统安全等级保护实施的总体流程

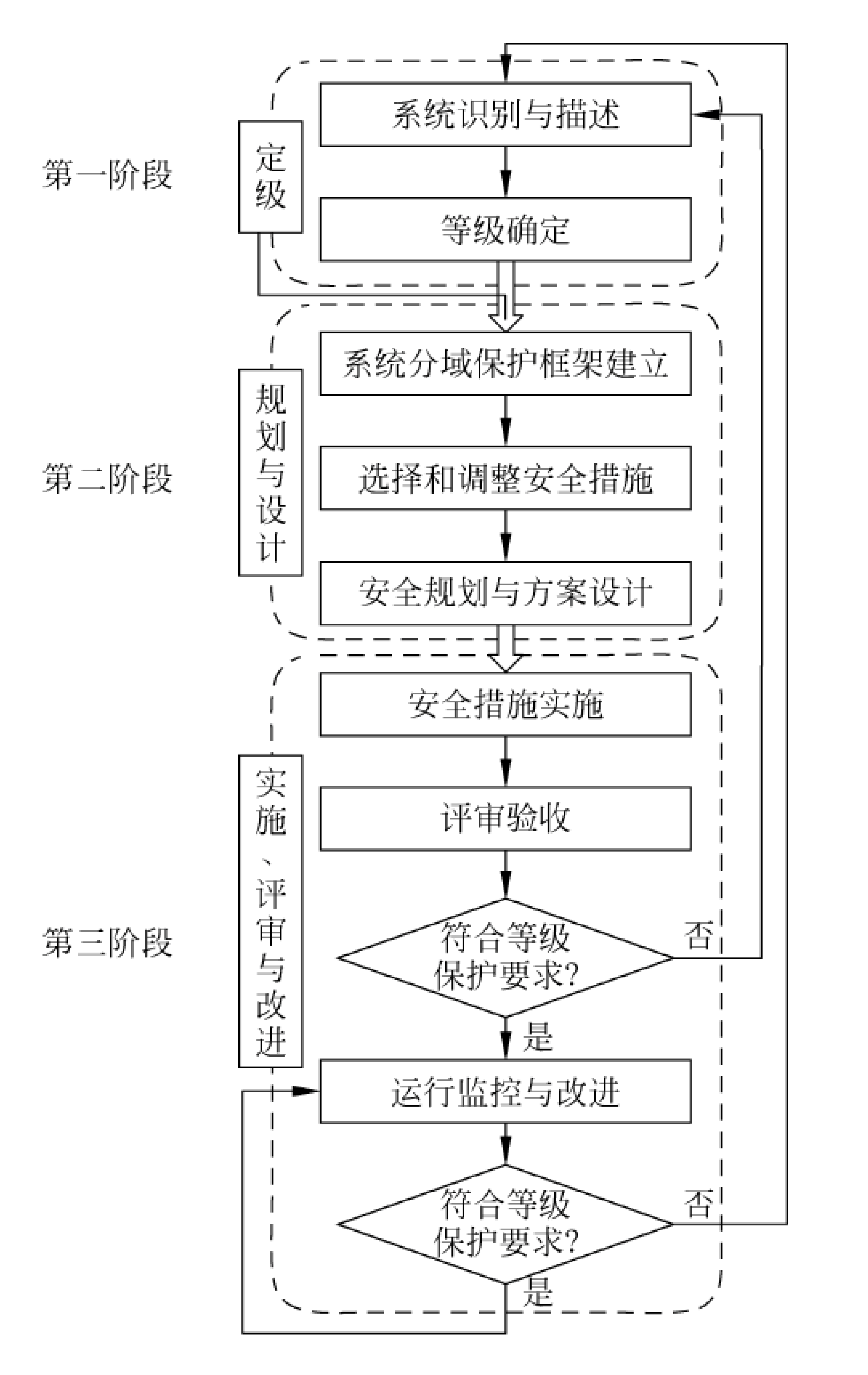


图 10-3　等级保护的基本流程

(1) 第一阶段，定级。主要包括以下两个步骤。

① 系统识别与描述：根据需要将复杂系统进行分解，描述系统和子系统的组成及边界。

② 等级确定：完成信息系统总体定级和子系统的定级。

(2) 第二阶段，规划与设计。主要包括三个步骤，分别如下。

① 建立系统分域保护框架：通过对系统进行安全域划分和保护对象分类，建立系统的

分域保护框架。

② 选择和调整安全措施：根据系统和子系统的安全等级，选择对应等级的基本安全要求，并根据风险评估的结果，综合平衡安全风险和成本，以及各系统特定安全要求，选择和调整安全措施，确定出系统、子系统和各类保护对象的安全措施。

③ 安全规划和方案设计：根据所确定的安全措施，制定安全措施的实施规划，并制定安全技术解决方案和安全管理解决方案。

(3) 第三阶段，实施、评审与改进。主要包括三个步骤，分别如下。

① 安全措施的实施：依据安全解决方案，建设和实施等级保护的安全技术措施和安全管理措施。

② 评估与验收：按照等级保护的要求，选择相应的方式来评估系统是否满足相应的等级保护要求，并对等级保护建设的最终结果进行验收。

③ 运行监控与改进：运行监控是在实施等级保护的各种安全措施之后的运行期间，监控系统的变化和系统安全风险的变化，评估系统的安全状况。如果经评估发现系统及其风险环境已发生重大变化，新的安全保护要求与原有的安全等级已不相适应，则应进行系统重新定级。如果系统只发生部分变化，例如发现新的系统漏洞，而这些改变不涉及系统的信息资产和威胁状况的根本改变，则只需要调整和改进相应的安全措施。

10.2　ISMS 与等级保护

1. 信息安全等级保护制度和 ISO/IEC 27000 系列标准的概念

从信息安全标准的发展实践看，大体从 20 世纪 90 年代前的想到要管什么，就制定什么标准的零星追加的发展阶段，发展到系统的、对一个信息系统的安全管理任务全面的、考虑一个体系结构，把谁来管(管理主体)，管什么(管理客体对象)，怎么管(组织的目的、要求、思想、方法)，靠什么管(组织环境或条件、过程、活动和工具)，管得怎么样(管理能力和效果的测度)，是否符合法规标准要求(管理审核)等问题给出一个通盘的规范性的指导，使管理行为可规划、可重复、可比较、可验证、可改进提高。使管理活动的计划、组织、领导、控制等关键环节有章可循，有据可查。

我国于 1999 年发布了国家标准 GB 17859《计算机信息安全保护等级划分准则》，成为建立安全等级保护制度、实施安全等级管理的重要基础性标准。目前已发布 GB/T 22239、GB/T 22240、GB/T 20270、GB/T 20271、GB/T 20272 等配套标准十余个，涵盖了定级指南、基本要求、实施指南、测评要求等方面，其中 GB/T 22080—2008 属于体系的要求，GB/T 22081—2008 是控制措施的实施指南。GB 17859 的核心思想是对信息系统特别是对业务应用系统安全分等级、按标准进行建设、管理和监督。2008 年，中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会正式发布了 GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》，公安部、国家保密局、国家密码管理局和国务院信息办等部门联合出台了信息安全等级保护工作的实施意见和管理办法等相关文件，大大加快了推进信息安全等级保护工作的开展。GB/T 22239—2008 是实施等级保护制度的基本要求，它针对每个等级的信息系统提出了相应的安全目标和安全保护要求。国家对信息安全

等级保护工作运用法律和技术规范逐级加强监管力度，保障重要信息资源和重要信息系统的安全。

ISO/IEC 27000 起源于英国的 BS 7799 标准系列，其中 ISO/IEC 27001 定名为《信息技术 安全技术 信息安全管理体系 要求》，已于 2005 年 10 月正式发布，是在组织内部建立信息安全管理体系(ISMS)的一套规范，其中详细说明了建立、实施、运行、监视、评审、保持和改进信息安全管理体系的模型和要求。它基于风险管理的思想，旨在通过持续改进的过程(PDCA 模型)使组织达到有效的信息安全，可用来指导相关人员应用 ISO/IEC 27002，通过规范的过程，建立适合组织实际要求的信息安全管理体系，实现其最终目的。ISO/IEC 27002 提出了在组织内部启动、实施、保持和改进信息安全管理的指南和一般原则，包括 11 个方面、39 个控制目标和 133 种控制措施。一个组织按照该标准实施其 ISMS 的过程中，依据 ISO/IEC 27002 的推荐选择控制措施，使用和 ISO 9001、ISO 14001 相同的管理体系过程模型。ISO/IEC 27004《信息技术 安全技术 信息安全管理测量》标准给出了测量组织 ISMS 实施有效性、过程有效性和控制措施有效性的过程和方法。

信息安全等级保护和 ISO/IEC 27000 系列标准是目前国内主流的两个信息安全管理标准体系。信息安全管理体系的建立是为了保障组织的信息和信息系统的安全，与等级保护的最终目标是一致的，虽然信息安全管理体系的名为管理，实际上涵盖了所有对技术实施方面的要求，是一个综合的管理体系。下面分别分析两者在出发点、分级标准、安全分类标准、实施流程及风险处理思想方面的共性与差异。

2. 等级保护系列标准与 ISO/IEC 27000 系列标准的共性

两者风险处理思想相同。信息安全没有百分之百的安全，所以无论是等级保护还是 ISO/IEC 27001 标准都在实施之前强调分级分类，只有找出信息安全保护的重点，才能把有限的资源投入到信息安全的关键部位，做到统筹安排。等级保护制度作为信息安全保障的一项基本制度，重点在于对信息系统进行分类分级。ISMS 是由信息安全最佳惯例组成的实施规则，主要从安全管理角度出发，提倡对信息系统进行风险评估，重点在于建立安全方针和目标，通过各种要素的相互作用实现这些方针和目标，并实现体系的持续改进。

控制措施是 ISMS 与等级保护制度中的重要内容，在控制措施的描述上，两者整体结构相近。ISO/IEC 27002 将控制措施的结构描述为控制类别－控制目标－控制措施－实施指南，而等级保护制度考虑了等级的概念，体现了不同等级信息系统的不同安全目标和不同安全要求，GB/T 22239—2008 结构的特点是安全目标－安全要求。

GB/T 22239—2008 将安全目标和安全要求都划分为两部分：技术方面和管理方面，技术方面包括物理安全、网络安全、主机系统安全、应用安全和数据安全，而管理方面则包括安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理，这 5 个方面贯穿了信息系统的全生命周期。在实际的技术要求中，也涉及管理的内容，比如在物理安全层面中对机房的管理、主机安全等层面中对安全审计的要求等。因此，等级保护中的管理与技术两大类是密不可分的，其具有相互关联性，能够在某些方面互相弥补，是一个统一的整体。

ISMS 的控制措施则主要考虑不同的类别，不同类别中有不同的控制目标和控制措施。ISO/IEC 27001 将控制措施划分为 11 个安全类别，分别为安全方针、信息安全组织、资产管理、人力资源安全、物理和环境安全、通信和操作管理、访问控制、信息系统获取开发和维护、

信息安全事故管理、业务连续性管理、符合性，进一步划分为若干安全目标和若干控制措施。

信息安全管理体系中，信息安全方针的管理与等级保护制度要求中的“安全管理制度：管理制度”的要求相同；在信息安全组织类中，信息安全管理的承诺对应“安全管理机构：岗位设置”、“安全管理制度：制定和发布”；信息安全协调对应“安全管理机构：沟通和合作”；信息安全职责的分配对应“安全管理机构：岗位设置”；信息处理设施的授权过程对应“系统建设管理：产品采购和使用”，保密性协议对应“人员安全管理：人员录用”，与政府部门的联系对应“安全管理机构：沟通和合作”；与特定利益集团的联系对应“安全管理机构：沟通和合作”；信息安全的独立评审对应“安全管理制度：制定和发布”；与外部各方相关风险的识别、处理与顾客有关的安全问题对应“人员安全管理：外部人员访问管理”；处理第三方协议中的安全问题对应“系统建设管理：安全服务商选择”。

在资产管理安全类中，资产清单、资产责任人、资产的合格使用、信息分类指南、信息的标记和处理对应“系统运维管理：资产管理”；人力资源安全类中，任用前的角色和职责对应“安全管理机构：人员配置”、“安全管理机构：岗位设置”；任用前的审查、任用条款和条件、人员任用中的管理职责对应“人员安全：人员录用”；信息安全意识、教育和培训对应“人员安全管理：安全意识教育和培训”；纪律处理过程对应“人员安全管理：人员考核”；任用终止职责、资产的归还、撤销访问权对应“人员安全管理：人员离岗”。

物理安全管理类中，大部分内容对应等级保护要求中的“物理安全”层面，其中物理安全边界、物理入口控制、办公室、房间和设施的安全保护、在安全区域工作、支持性设施、资产的移动对应“系统运维管理：环境管理”；设备维护、组织场所外的设备安全对应“系统运维管理：设备管理”；设备的安全处置和再利用对应“系统运维管理：介质管理”。

在通信和操作管理安全类中，文件化的操作程序对应“安全管理制度：管理制度”中日常操作规程的要求；变更管理对应“系统运维管理：变更管理”；系统操作的责任分割对应“安全管理机构：人员配置”；开发、测试和运行设施分离对应“系统建设管理：自行软件开发”；第三方服务交付对应“系统建设管理：系统交付”；第三方服务的监视和评审对应“系统建设管理：工程实施”中关于实施过程管理、建立等方面的要求；第三方服务的变更管理对应“系统运维管理：变更管理”中关于系统变更的控制；系统容量管理对应“系统运维管理：系统安全管理”中关于系统容量的要求；系统验收对应“系统建设管理：测试验收”和“系统建设管理：系统交付”；控制恶意代码、控制移动代码对应“系统运维管理：恶意代码防范”；信息备份对应“系统运维管理：备份与恢复管理”；网络控制对应“系统运维管理：网络安全管理”；网络服务安全对应的是等级保护技术要求中的网络安全层面；可移动介质的管理、介质的处置对应“系统运维管理：介质管理”；系统文件安全对应“系统运维管理：系统安全管理”；审计日志对应“系统运维管理：系统安全管理”；监视系统的使用对应“系统运维管理：监控管理和安全管理中心”；另外一些如日志信息的保护、管理员和操作员日志、故障日志、时钟同步、电子消息发送、业务信息系统、电子商务、在线交易等对应到等级保护要求中的“主机安全”、“应用安全”、“数据安全”等多个层面。

在访问控制安全类里面，大部分都对应着等级保护要求的“主机安全”、“应用安全”、“网络安全”中的“访问控制”控制点。另外，访问控制策略对应“系统运维管理：系统安全管理”；网络连接控制对应“系统运维管理：网络安全管理”。

系统安全要求分析和说明对应“系统建设管理：安全方案设计”；密钥管理对应“系统

运维管理：密码管理”；变更控制程序、操作系统变更后应用的技术评审对应“系统运维管理：变更管理”；外包软件开发对应“系统建设管理：外包软件开发”；技术脆弱性的控制对应“系统运维管理：网络安全管理”和“系统运维管理：系统安全管理”中关于系统漏洞及补丁的要求。

在信息安全事件管理的安全类里面，报告信息安全事态、报告安全弱点、职责和程序、对信息安全事件的总结、证据的收集都对应着“系统运维管理：安全事件处置”。

在业务连续性管理安全类中，主要对应等级保护要求中的“系统运维管理：应急预案管理”，但是业务连续性管理中提到了要进行风险评估，并根据评估结果开发连续性计划，这与等级保护政策中开展等级测评，并根据测评结果进行信息系统改建的要求是相一致的。

在符合性要求类中，主要涉及等级保护要求中的“安全管理机构：审核和检查”及一些技术要求。

3. 等级保护系列标准与 ISO/IEC 27000 系列标准的差异性

首先，两者的出发点不同。信息安全等级保护制度是以国家安全、社会秩序和公共利益为出发点，从宏观上指导全国的信息安全工作，目的是构建国家整体的信息安全保障体系，ISO/IEC 27000 系列标准是以保证组织业务的连续性，缩减业务风险，最大化投资收益为目的，目的是保证组织的业务安全。

其次，两者的分级标准存在差异。等级保护实施首先是定级问题，针对不同的级别，提出了不同的等级安全要求；ISO/IEC 27000 系列标准的第一步是风险评估，根据资产的价值和所面临的风险进行分类，然后针对不同的风险选择相应的风险处置措施。虽然都是从分级或分类入手，但是两者的分级标准不同。等级保护的分级主要考虑 4 个方面的风险，即信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益所造成的影响，按照影响程度大小分为 5 级，等级保护的分级以组织外部影响为依据。而 ISO/IEC 27000 系列标准的分级是根据资产、威胁、脆弱点、影响、风险等各个因素之间的关系，采取定量或者定性的方法进行分级分类，采取何种风险处置措施，也是组织根据自己对风险的接受程度而决定。ISO/IEC 27000 标准以组织内部业务影响为依据。

两者的安全分类上存在差异。等级保护和 ISO/IEC 27000 系列标准都从技术和管理两个方面提出了信息安全的要求。等级保护有 10 个方面的要求，技术方面有物理安全、网络安全、主机系统安全、应用安全、数据安全，管理方面有安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理；而 ISO/IEC 27001 标准有 11 个方面，分别是：安全策略、组织信息安全、资产管理、人力资源安全、物理和环境安全、通信和操作管理、访问控制、信息系统获取开发和维护、信息安全事件管理、业务连续性管理、符合性。而且两者在各个大分类下面又规定了若干的小项目。

两者在实施流程上存在差异。等级保护首先对信息系统进行定级，定级之后再结合不同等级的安全要求进行安全需求分析。在定级之前，首先要对信息系统进行描述，主要包括系统边界、网络拓扑、设备部署等，对于大型的信息系统要在综合分析的基础上进行划分，确定可作为定级对象的信息系统个数。信息系统的定级由受侵害客体和对客体的侵害程度两个因素决定，通过综合判定客体的受侵害程度来确定系统的安全保护等级。安全等级确定之后，从信息系统安全等级保护基本要求中选择相应的等级评价指标，通过现场观察、询问、

检查、测试等方式进行评估，确定信息系统安全保护的基本需求。对于有特殊保护要求的信息系统重要资产，其安全需求分析则采用风险评估的方法来进行。ISO/IEC 27000 系列标准通过风险评估来识别风险和威胁，进而确定组织的信息安全需求，选择风险控制措施。在风险评估之前首先根据组织业务特征、资产和技术来确定 ISMS 范围和 ISMS 方针，然后选择使用于组织的风险评估方法，识别 ISMS 范围内的资产、资产所有者、资产的威胁、可能被资产利用的脆弱点、资产损失可能造成的影响，对风险进行分析和评价，评估安全失效可能造成的影响及后果、威胁和脆弱性发生的可能性，进而确定风险的等级。整个风险评估的过程就是对组织信息安全需求分析的过程。

10.3　等级保护与风险评估

10.3.1　风险评估是等级保护制度建设的基础

信息系统安全等级保护是国家信息安全基本制度，信息安全风险评估是科学的方法和手段。制度的建设需要科学方法的支持，方法的实现与运用要体现制度的思想。因此，在等级保护制度建设的过程中，风险评估作为一项科学的手段和方法对等级的确定、建设和维护进行技术支持；同时，在风险评估中，对资产、威胁、脆弱性以及风险等各要素识别及赋值时，进行了 5 级划分以体现等级的思想。两者是密不可分的。

等级保护究其实质是根据信息系统的实际情况，结合组织或机构的客观需求，综合考虑风险控制成本与风险造成的影响，采取具有不同保护强度的安全措施，并将风险控制在可接受的范围内。

信息系统安全等级保护制度在建设中要涉及一系列技术问题。对于不同系统的安全域，运用何种强度的安全保护措施、措施的有效性是否能够达成、如何调整措施以满足系统的安全需求等，都可通过风险评估的结果来进行判断与分析。整个过程包括等级的确定、等级的建设和等级的维护三个阶段。

1. 等级的确定

依据信息安全风险评估国家标准对所评估资产的重要性、客观威胁发生的频率以及系统自身脆弱性的严重程度进行识别和关联分析，判断信息系统应采取什么强度的安全措施，才能够将安全事件一旦发生后可能造成的影响控制在可接受的范围内。即依据风险评估的结果来确定信息系统安全措施的保护级别。

2. 等级的建设

根据信息系统安全等级保护国家标准的要求，从管理与技术两个方面选择不同强度的安全措施，并依据有关技术要求对安全措施的功能的达成进行符合性测试，以确保建设的安全措施满足相应的等级要求。

3. 等级的维护

等级的维护包括两方面：一是维护现有安全措施的等级的有效性，可依据国家有关标

准对信息系统所采取的安全措施是否满足相应等级的要求进行符合性测试，以保证所采取的安全措施的强度的持续有效；二是根据客观情况的变化以及系统内部建设的实际需要，等级要进行定期的调整，以防止过度保护或保护不足，再定级的过程可参见等级的确定部分的内容。

10.3.2 等级保护和风险评估的宏观联系

信息系统安全等级保护制度作为我国信息安全保障体系建设的一项基本制度，它的总体目标是为了统一信息安全保护工作，提高我国信息安全建设的整体水平。通过充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到对信息和信息系统重点保护和有效保护的目的。等级保护工作的核心是对信息系统安全分等级，按标准进行建设、管理和监督。

风险评估是基于传统的风险管理经验通过对信息系统的资产、威胁、弱点和风险等要素进行评估分析的过程。信息系统的用户常常借助风险评估方法来分析自己的安全现状，评估自身安全需求和安全现状的差距，从而进行安全整改。

等级保护制度从一定意识上讲是信息安全保障工作中国家意志的体现，体现了国家对相应系统建设和使用单位在信息安全建设方面的基本要求。风险评估作为信息安全工作的一种重要技术手段，在实施信息安全等级保护周期和层次中发挥着重要作用。

在落实信息系统安全等级保护工作中，信息系统运营使用单位可以结合本单位信息系统应用及行业特点，自主开展系统风险评估，为等级保护的定级、测评和整改等工作阶段提供重要参考依据。

10.3.3 风险评估是信息系统安全等级保护的技术支撑

信息系统安全等级保护是建立在风险评估的基础之上的。风险评估是信息安全等级保护的基础。从风险评估的思想出发，对深刻地理解等级保护原理与实质是非常有意义的。

1. 信息系统等级划分与资产的识别

在公通字[2004]66 号关于印发《关于信息安全等级保护工作的实施意见》的通知中，根据信息和信息系统的重要程度，将信息和信息系统划分为 5 个等级：自主保护级、指导保护级、监督保护级、强制保护级和专控保护级。

实际上，对信息系统的定级过程，也就是对信息资产的识别及赋值的过程。

在国家的《定级指南》中，提出了对信息系统的定级依据，而这些依据基本的思想是根据信息资产的机密性、完整性和可用性重要程度来确定信息系统的安全等级，这正是风险评估中对信息资产进行识别并赋值的过程：对信息资产的机密性进行识别并赋值；对信息资产的完整性进行识别并赋值；对信息资产的可用性进行识别并赋值。

从某种意义上来说，信息系统的安全等级划分，实际上也是对残余风险的接受和认可。信息系统的风险是普遍存在的，可以通过技术的、管理的手段对风险加以控制、转移、部分清除。但是，不可能也没有必要完全消除风险，零风险是不存在的，也没有必要去追求。通过各种手段进行保护以后，必定还会有一定的残余风险。这部分风险一方面是没有发现的，另

一方面，可能是经过分析之后，认为是可以接受的。而不同安全等级的信息系统，可接受的残余风险是不同的，程度也是不一样的。在信息系统的生命周期内，对于残余风险，应该实时地进行监控和评估，以防止可能导致的安全事件的发生。

2. 安全等级的要求

在等级保护中，对系统的定性完成后，应该按照信息系统的相应等级提出相应的安全要求，安全要求实际上体现在信息系统在对抗威胁的能力与系统在被破坏后，恢复的速度与恢复的程度方面。而这些在风险评估中，则是对威胁的识别与赋值活动；脆弱性识别与赋值活动；安全措施的识别与确认活动。

GB 17859 等标准没有从威胁的角度提出对信息系统的安全要求，而是单纯地从消除脆弱性角度提出了信息系统的安全要求。对于一个安全事件来说，是威胁利用了脆弱性所导致的，在没有威胁的情况下，信息系统的脆弱性不会自己导致安全事件的发生。所以对威胁的分析与识别是等级保护安全要求的基本前提。不同安全等级的信息系统应该能够对抗不同强度和时间长度的安全威胁，如在 DDoS 攻击中，安全等级较高的信息系统不仅能够对抗来自个体攻击源的入侵，甚至能够对抗大规模僵尸网络的长时间的攻击。这实际提出了对信息系统的脆弱性的要求，抗攻击能力，实际是信息系统本身的强度所在。应该以威胁为前提，提出各等级相应的保护能力的要求。

3. 安全设计首先应该以风险评估的结果为依据

在确定信息系统的安全等级和进行风险评估后，应该根据安全等级的要求和风险评估的结果进行安全方案设计，而在安全方案设计中，首要的依据是风险评估的结果，特别是对威胁的识别，在一些不存在的威胁的情况下，对相应的脆弱性应该不予考虑，只作为残余风险来监控，而不应该理会安全等级的要求是如何规定的。

安全等级的要求，是面向所有需要保护的信息系统的，不可能针对某一个信息系统提出，是共性的，而不可能是个性的。一个信息系统，具有自己的个性化特点，这些个性化特点必须在保护中使用合理的策略进行保护。对于两个等级相同的信息系统，由于所承载业务的不同，其信息的安全属性也可能不同，对于需要机密性保护的信息系统，和对于一个需要完整性保护的信息系统，保护的策略必须是不同的。所以，安全设计首先应该以风险评估的结果作为依据，将设计的结果与安全等级保护的要求相比较，并符合安全等级要求。

10.3.4　风险评估在等级保护周期中的作用

信息系统安全等级保护制度在建设中要涉及一系列技术和管理问题。对于不同系统的各个安全域，用什么样强度的安全保护措施、措施的有效性是否能够达成、如何调整措施以满足系统的安全需求等，都可通过一些手段和方法来进行判断与分析。风险评估作为用户自主的一种技术手段可以运用到等级保护周期的系统定级、安全实施和安全运维三个阶段。

1. 系统定级

由于信息系统具有自身的行业和业务特点，且所受到的安全威胁均有所不同，因此，可以依据信息安全风险评估国家标准对所评估资产的重要性、客观威胁发生的频率以及系统

自身脆弱性的严重程度进行识别和关联分析，判断信息系统应采取什么强度的安全措施，然后将安全事件一旦发生后可能造成的影响控制在可接受的范围内。即将风险评估的结果作为确定信息系统安全措施的保护级别的一个参考依据。

2. 安全实施

安全实施是根据信息安全等级保护国家标准的要求，从管理与技术两个方面选择不同强度的安全措施，来确保建设的安全措施满足相应的等级要求。风险评估在安全实施阶段就可以直接发挥作用，那就是对现有系统进行评估和加固，然后再进行安全设备部署等。在安全实施过程中也会发生事件并可能带来长期的安全隐患，如安全集过程中设置的超级用户和口令没有完全移交给用户、防火墙部署后长时间保持透明策略等都会带来严重的问题，风险评估能够及早发现并解决这些问题。

3. 安全运维

安全运维是指按照系统等级进行安全实施后开展运行维护的安全工作。安全运维包括两方面：一是维护现有安全措施等级的有效性。可依据国家有关等级划分准则对信息系统所采取的安全措施是否满足要求进行检验，以保证所采取的安全措施的强度持续有效；二是根据客观情况的变化以及系统内部建设的实际需要，等级要进行定期调整，以防止过度保护或保护不足。再定级的过程可参见系统定级部分的内容。

等级保护的三个阶段和风险评估的关系如图 10-4 所示。

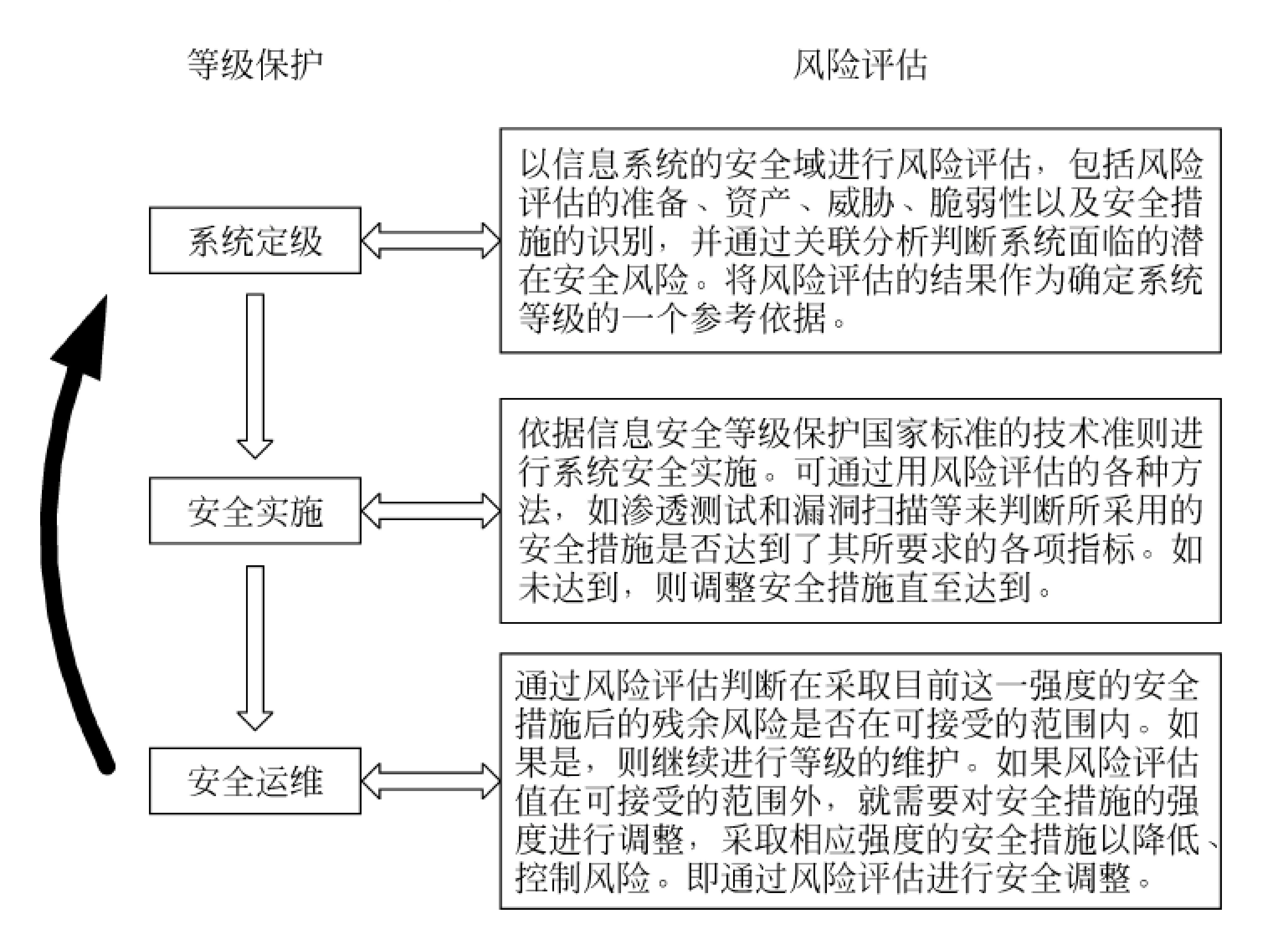


图 10-4 等级保护的三个阶段和风险评估的关系

从图中可以看出，在等级保护的三个环节中，风险评估的作用分别为：在系统定级阶段用于参考帮助确定系统的安全等级；在安全实施阶段可以作为评估系统是否达到必需的安全等级的重要依据；在安全运维阶段开展定期和不定期风险评估以便帮助确认它保持的安全等级是否发生变化。

10.3.5　风险评估在等级保护层次中的应用

风险评估不但在等级保护周期的各阶段发挥着重要的作用，在等级保护的各层次中也不可或缺。下述简单列出了风险评估的技术手段示例在等级保护的各层次中发挥的作用：

（1）漏洞扫描可以大致分为如下4类：主机漏洞扫描、网络漏洞扫描、数据库漏洞扫描、应用漏洞扫描。它们分别可以应用在等级保护中的主机安全、网络安全、数据库安全、应用安全的技术要求部分。

（2）系统审计可以应用在等级保护中的网络安全审计、主机安全审计、数据库安全审计、应用安全审计的技术要求部分。

（3）渗透测试可以应用在等级保护中的安全方案实施和安全运维两个阶段，并在网络安全、主机安全、应用安全、数据安全等技术要求部分起着辅助作用。

思考题

1. 叙述我国信息系统安全等级保护标准体系的发展历程。
2. 解释等级保护的原则。
3. 叙述信息系统安全保护等级划分与不同等级的安全保护能力。
4. 试述等级保护的基本流程。
5. 归纳ISMS与等级保护的关系。
6. 归纳风险评估与等级保护的关系。

第11章 云计算的安全管理与风险评估

11.1 云计算概述

1. 云计算的概念

云计算是信息时代网络计算技术的组织、应用与服务方式的创新模式，目前还没有统一的标准定义。从用户的视角来看，云计算是可以随时随地使用任何一种电子终端接入所需应用的一种服务，不管是用手机还是计算机等，是一种服务的交付和使用模式，用户（包括个人、企业或其他组织等）通过网络以按需、易扩展的方式获得所需的服务。从 IT 视角来看，云计算是并行计算（Parallel Computer）、分布式计算（Distributed Computing）和网格计算（Grid Computing）的发展，是以虚拟化技术为基础的、近年来新技术的整合应用，是并行计算、分布式计算、网格计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物，可以提供可测量、按需的服务。美国国家标准技术研究所（NIST）将云计算定义为：软件、平台和基础设施的服务化，并依据部署方式的不同分为私有云、公共云等不同的类型。我国的一个看法，认为云计算是一种基于互联网的、大众参与的计算模式，提供动态的、虚拟化的服务，其计算资源包括计算能力、存储能力、交互能力等。

云计算就是将计算任务分布在由大量计算机构成的资源池上，使各种应用系统能够根据需要获取计算能力、存储空间和各种软件服务，其各种资源往往是动态变化的，通常是通过互联网以服务的形式提供给用户，而用户并不清楚“云”中的具体技术架构。云计算的底层结构包括数据中心（Data Center）提供的可靠服务和建立在不同虚拟技术之上的服务器。数据中心可以提供各种可靠的服务，云计算核心是服务，强调软件即服务（Software as a Service，SaaS）、平台即服务（Platform as a Service，PaaS）、基础设施即服务（Infrastructure as a Service，IaaS）等，借助 SaaS、PaaS、IaaS 等先进的商业模式把强大的计算能力提供给终端用户。

2. 云计算模式

云计算作为一种服务供应链，是云计算服务运营商和众多服务提供商等不同利益主体的合作型系统。它具有如下特点：比传统的供应链更加不稳定；属于技术性的网络服务产品；服务产品具有易逝性；自身利益的最大化与其他成员或与系统整体目标产生冲突。图 11-1 给出了云计算典型的计算模式示意图。

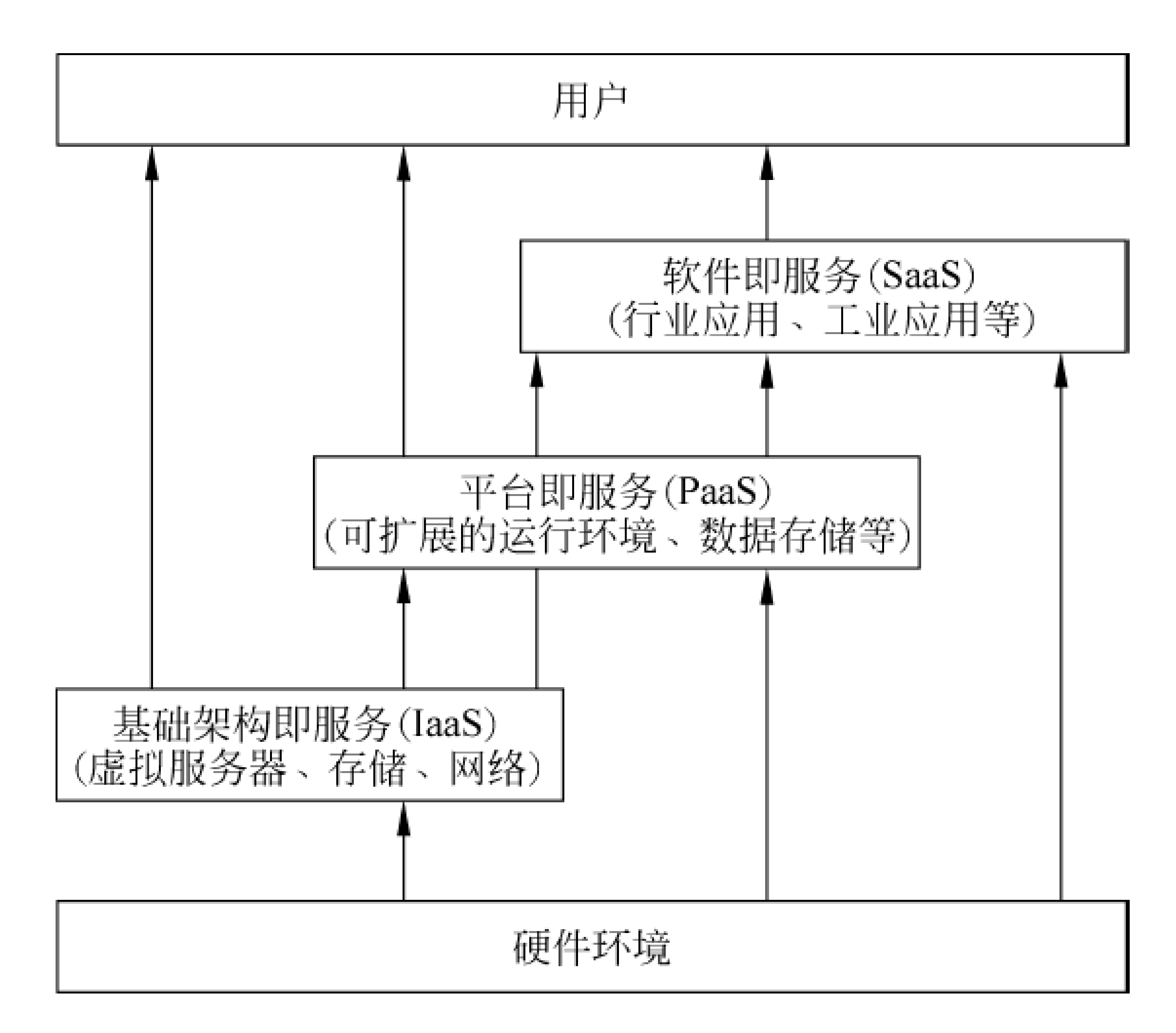


图 11-1　云计算典型的计算模式示意图

构成云计算的组成架构包括用户层、接入环境、计算环境层和管理平台层，如图 11-2 所示。

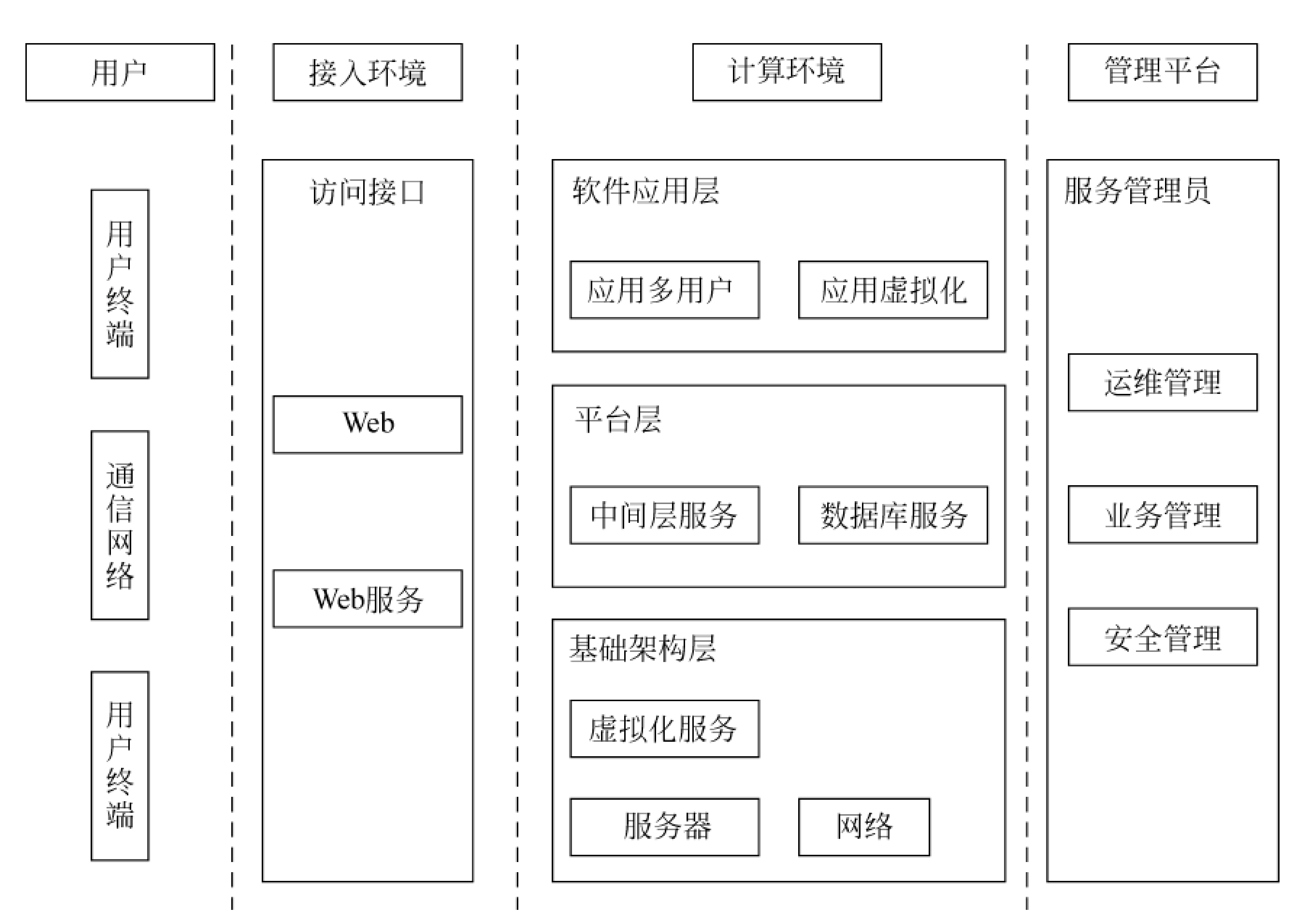


图 11-2　云计算组成架构

云计算的特点通常包括以下内容：

(1) 超大规模，包括无限多的空间、强大的计算。

(2) 虚拟化。

(3) 高可靠性，包括数据存储的高可靠性。

(4) 高可扩展性。

(5) 服务面向的广泛性。

(6) 按需服务。

(7) 极其廉价,包括服务价格、用户端设备成本。

(8) 用户计算的分布性。

(9) 通用、且使用方便。

(10) 轻松实现不同设备间的数据共享。

11.2 云计算的信息安全问题

云计算是一种能够动态伸缩的虚拟化资源,是通过网络以服务的方式提供给用户的计算模式,用户不需要知道如何管理云计算的基础设施。亚马逊(Amazon)、Google、微软等知名 IT 公司推出云计算策略和服务,各大公司在云计算业务领域的竞争正逐渐加剧。云计算给我们带来诸多好处的同时,也带来了相应的信息安全方面的挑战。基于云计算的信息安全事件时有发生。2009 年,亚马逊的云存储出现故障、持续时间约 4h,谷歌公司尴尬地承认了不小心泄漏客户私人信息的事实,微软在博客中发布了微软云计算平台 Windows Azure 运作中断的消息等。其安全风险在于:由不可控、不可信的云经营商统管 IT 资源和计算基础设施,更大规模异构共享和虚拟动态的运营环境难以控制。

云计算平台集中有大量用户的数据和应用,因而同时面临着传统的网络安全问题,如恶意的攻击、访问权限控制、数据备份、数据意外丢失、网络传输安全等。除此之外,云计算所面临的新的安全问题大致包括以下几个方面。

(1) 传统的安全边界消失、虚拟化服务的安全问题。传统的信息安全技术、网络安全技术、加密与密钥管理、安全审计等技术,为适应云计算服务模式在技术实现上提出了新的挑战。

(2) 数据集中后的安全问题。云服务商可能以用户未知的方式越权访问或使用用户数据;当用户的隐私被侵犯时,云服务提供商是否支持并帮助用户进行调查。

(3) 稳定性、可靠性及服务连续性问题。当自然灾害、硬件设施遭到损坏和故障等情况发生时,云计算提供商是否有相应的措施来保障正常的服务;当云计算服务商破产或兼并重组后,用户的数据会不会受到影响。

(4) 云计算服务提供商、云计算的信任问题。包括 Google、微软、IBM、亚马逊在内的各个云计算供应商都有一套自己的标准,彼此互不兼容,提供的服务内容也不尽相同。当前云服务商基本上是以用户不可见的方式提供计算处理或数据存储的服务,缺乏透明度,对于用户来说可能存在未知的风险。

(5) 云计算的数据安全性问题。从用户使用的安全角度来看,存在一个透明度的问题。由于用户数据都在云里面,数据的丢失、篡改是用户无法控制的,同时还涉及隐私的保护。

(6) 云计算面临潜在的机密性问题。多主租用架构要求不同的用户分享基础设施、服务和应用等,如何做到相互隔离,防止用户有意或无意的"越轨"行为;由于用户的程序是运行在数据中心之内的,需要预防恶意用户从云计算平台内部发起攻击。

(7) 数据存储风险和信息主权挑战:我们已经看到了类似 Google Gmail 用户隐私泄漏的问题以及亚马逊宕机等事件的发生,所以不排除某些国家或云服务提供商也会在需要的

时候,利用云计算损害其他国家的利益。

(8) 云计算安全缺乏标准。从技术上来说,由于现在云计算没有国际或行业的标准,技术或服务提供商提供了不同的 API,如何实现它们之间互联互通还缺少技术规范,云计算的标准化是亟待解决的问题。此外,管理和运行云计算也是一个难点。已有的管理或运行规范,如 ISO/IEC 27000 系列、ISO 20000 等标准是否适合云计算服务还值得研究。

(9) 相关的法律法规不完善。当信息储存在自己的计算机中时,法律保障任何人都需要经过本人的允许才能合法地查看这些信息。而当信息储存在云中时,并没有明确的法律规定服务方或政府不能查看这些信息;当前云计算服务供应商在服务协议中尽可能地规避了大部分风险问题,不承诺对任何数据泄密及数据被破坏行为承担法律责任或义务,云服务提供商的服务水平协议(SLA)存在“霸王条款”嫌疑。如 2011 年亚马逊连续 4 天的宕机故障竟然并没有违反和用户签订的服务水平协议;在云计算中,数据存储常常分布在不同的国家或地区。假设中国的用户使用了美国云计算服务商提供的服务,但是数据却保存在加拿大的数据中心,如果此时出现法律纠纷,如何去保护中国用户的利益存在困境,因为不同的国家都可能会声称对数据拥有司法权或者访问权,这时需要国际上进行统一协调,可以通过签订双边或多边的协定、最好是制定一个全球法律协议来保障各方的利益。云计算安全治理同样是一个很重要的问题,对各国法规遵从性、电子司法取证等提出了相应的挑战。

尽管云计算存在以上安全问题,但这只是云计算成长中的经历。对用户来说,更重要的是增强安全意识,及早发现并采取必要的防范措施来确保安全。这就要求人们进行定期、不定期有效的信息安全风险评估。因此,建立一套基于云计算的信息安全风险评估办法是十分必要的。

11.3　云计算的风险评估与控制措施

11.3.1　云计算的风险评估

信息安全风险评估是指依据有关信息安全管理标准和技术,对信息系统及其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行评价的过程。风险评估人员实施评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性,结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响,提出有针对性的抵御威胁的防护对策和整改措施。

充分了解云计算的服务模式对云计算的信息安全风险评估是十分必要的。云计算中数据的处理、传输和存储都依赖于互联网和相应的云计算平台,数据和应用程序并不需要一定在同一地点,风险评估要素和方法与传统的信息安全风险评估有所不同,需要考虑云安全设施、云存储设施、服务水平协议(SLA)、合同需求及提供商文档化等因素。Gartner 指出云计算技术存在 7 大风险:特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持、长期生存性。针对云计算的风险评估可以采取如下步骤:

1. 资产识别

(1) 确定把什么样的数据或功能迁移进云,有些资产在未来有可能也会牵涉到,它们也

应该被考虑在内。

(2) 确定数据或功能对于本组织的重要性。至少需要对涉及的应用、功能和过程的重要程度和资产的重要性有一个大致的评估。对于每项资产,要考虑遇到以下情况时将会受到什么影响或损害:

① 该项资产可能被广泛公布并广为散发。

② 云服务提供商的员工可能访问该项资产。

③ 该项功能或过程可能被外人操纵。

④ 该项功能或过程可能没有提供预期的结果。

⑤ 该项数据可能被意外更改。

⑥ 该项资产在一段时间内可能无法使用。

事实上,资产的机密性、完整性和可用性,以及如果全部或部分资产迁移到云中处理,这些安全性将会受到何种影响,这与评估一个潜在的外包项目类似,只是对于云计算,有各种部署选项以及内部模型。

(3) 将资产映射到可能的云部署模型。对资产的重要性有所了解后,下一步的工作是确定对哪些部署模式更感兴趣。在开始寻找服务提供商之前,应该了解各种不同部署模型带来的风险:公共云计算模型、私有云计算模型、社区云计算模型、混合云计算模型。至此,应能确定是否可以过渡到云、采用什么部署模型来满足安全和风险要求。

(4) 资产赋值。根据各项资产的重要程度对资产赋值,分别对资产的三个安全属性进行赋值:机密性、完整性和可用性。采取等级评定的方法,把各种属性划分为5个等级,分别用5、4、3、2、1表示很高、高、中等、低和很低,选择三个属性中最高赋值为该资产赋值。

2. 威胁识别

威胁是产生风险的外因,威胁识别包括威胁分类和威胁赋值。威胁可能来自故意或偶然的因素,这些因素通常包括人、系统和自然环境等。在云计算风险评估中,建议采用以下步骤:

(1) 评估可能的云服务模式和提供商。这一步的关注点是每个SPI(SaaS、PaaS、IaaS)层次上可能拥有的控制等级,以实现不同的风险管理要求。由于云计算中的按需提供和多租户特点,传统形式的审计和评估可能并不适用,例如,有些云服务商限制用户进行渗透测试,而有些则限制提供审计日志和实时监控数据。对这些因素带来的威胁的评估需要寻找替代的评估方法,或寻找与风险管理需求更一致的其他提供商。

(2) 画出潜在的数据流,找出威胁暴露点。对一个特定的部署选项,需要画出组织与云服务、客户和其他节点之间的数据流图,对可能存在的威胁进行分类,可以通过故障树分析法、层次分析法等方法进行分类。

(3) 根据威胁发生的频率进行赋值。可以通过威胁识别的结果确定被评估信息系统所面临的主要威胁。

3. 脆弱性的识别

脆弱性是产生风险的内因,本部分工作包括脆弱性识别和脆弱性赋值,需要明确云计算在技术上和管理上存在的漏洞。不同的云计算平台对应不同的基础架构,根据其规模、是否

允许特权用户的接入，计算平台的可审查性、数据位置、数据隔离措施、数据恢复措施及长期生存性等特性，识别可能引起安全事件的脆弱性；对于某一个特定的脆弱性，用 0 和 1 分别表示不存在和存在脆弱性。

11.3.2　云计算的安全措施

从诞生以来，云计算始终是 IT 行业最炙手可热的技术之一。现在，无论看网页、发微博、玩社交网站，还是搜索、发邮件、即时通信，包括在线支付，都不知不觉地使用了云计算。尽管云计算表现出了非凡的能力，但其自身的安全问题仍然导致公众对这种新兴技术心存疑虑。据国外权威调研公司的调查显示，20.9％的被调查者最关注的是云计算的安全和隐私问题。在过去的几年里，索尼视频游戏网站、国内程序员社区 CSDN 先后遭到黑客攻击、用户资料泄漏，就是其中的典型例子。针对云计算信息安全，典型的控制措施包括以下几个方面。

研究云计算服务供应链，从提升整体云服务供应链角度出发，研究统一的安全策略以及云计算服务供应链的风险分担机制，力求建立服务供应链的协调策略，促进服务供应链整体收益最大化。在随机需求环境下，合理的安全共享协调机制是云计算服务供应链稳定性和协调性的重要保证。同时，云服务运营商无法衡量和监控云服务供应商的努力程度，必须明确相关方的法律责任。

通过风险评估建立公共云和私有云。云端的安全防护不同于以往的防护，针对业务流隔离与用户隐私数据安全的两大障碍，企业用户在使用云计算中的服务之前，首先对企业数据和应用服务进行风险评估分析，在企业内部应该根据自身评估结果划分出公共云和私有云，根据服务的重要性划分等级。公有云缺少必要的安全防范，从本质上讲是不安全的。而且，所有基础设施、应用程序以及用户数据的维护完全依赖于云计算服务提供商，数据安全和隐私对用户来讲是不可控的。想在不安全且不可控的公有云上保护用户隐私，最彻底的解决方案是不把隐私数据放在公有云上，而是把这些数据放在用户可控的范围之内。如果隐私数据必须在公有云中处理，那么处理完后要及时删除。如果隐私数据必须被保存在公有云中，云计算服务提供商必须能够提供较高等级的安全性。前两种措施需要个人用户提高自身的保密意识，时时刻刻绷紧防泄密这根弦。企业用户还需要制定严格的数据保密制度，例如，根据数据隐私性和重要性划等级，最高等级的数据绝对不能放在“云”中，低一级的可以放在“云”中进行处理，但原始数据和处理结果必须从“云”中清除。对于第三种措施，选择一家可靠的云计算服务提供商至关重要。在选择运营服务商的时候，应该根据具体企业的具体应用要求来选择，一般选择规模比较大的、有信誉、品牌好、经营合理的大公司。一般而言，云计算服务提供商保护用户隐私数据的措施主要有访问控制、数据加密、使用安全协议、提高数据可用性 4 种。然而这些措施要么有一定的局限性，要么还在发展当中，都不能确实保证用户隐私数据万无一失。可以利用计算机取证和安全监控技术加强对云计算的监管，增强云计算的安全性：用户利用取证和监控工具对重要目标（虚拟主机、物理主机、敏感数据、网络流量等）实施监控，监控“云”中可能发生的异常行为。当网络安全事件发生时，马上进行应急响应取得证据，利用监控数据或电子证据追溯异常行为所产生的源头，为下一步司法介入铺平道路。这种方式以计算机取证和网络安全技术为基础，以法律为依托，将取证和法律手段引入云计算这个“虚拟社会”，维护云计算安全和秩序，避免用户的数据和隐私受

到侵害，也不失为一种有效的尝试。

借鉴可信任计算的思想，建立可信云。可信任计算是由可信任模块到操作系统内核层，再到应用层都建立关系，构建信任关系，并在此基础上，扩展到网络中建立起信任链，从而形成对病毒和木马的免疫。在云端，组成可信任链，通过可信任键的扩充组成可信任云。

构建可靠的虚拟化环境，确保云计算服务安全。“按需服务”是云计算平台的终极目标，而只有借助虚拟化技术，才有可能根据用户的需求，来提供个性化的应用服务和合理的资源分配。也就是说，无论是基础的网络架构，还是存储和服务器资源，都必须要支持虚拟化，才能提供给用户端到端的云计算服务。因此，秉承安全即服务的理念，在云计算数据中心内部，应采用 VLAN 和分布式虚拟交换机等技术，通过虚拟化实例间的逻辑划分，实现不同用户系统、网络和数据的安全隔离。应采用虚拟防火墙和虚拟设备管理软件为虚拟机环境部署安全防护策略，并对云计算系统的运行状态和进出的数据流量实施实时监控，及时发现并修复虚拟网络和系统异常。应采用防恶意软件，建立补丁和版本管理机制，防范因虚拟化带来的潜在安全隐患，确保虚拟化环境与物理网络环境一样安全、可靠。

综合应用多种技术手段，确保数据安全。数据的存储安全，确保用户信息的可用性、隐私性和完整性，是云计算安全的核心内容，无论是数据的加密、隐藏，还是数据资源的灾难备份等方面，都是围绕着数据安全展开的。因此，在云计算环境下，应采用数据加密技术，建立密钥管理与分发机制，实现用户信息和数据的安全存储与安全隔离，防止用户间的非法越权访问。加强数据的私密性可以保证云计算的安全，无论是用户还是存储服务提供商，都要对文件数据进行加密，这样既保证文件的隐私性，又可以进行数据隔离。应实施严格的身份监控、登录认证、权限控制和用户访问审计，实现用户信息和数据的高效维护与安全管理。安全认证包括单点登录认证、强制用户认证、代理、协同认证、资源认证、不同安全域之间的认证或者混合认证等方式，其中很多云计算提供商是通过结合强制用户认证和单点用户认证的方式来实施对用户进入云应用的认证，用户只需登录一次进入整个云计算应用，从而可以有效地避免用户在使用自己的服务时将密码泄漏给第三方。应完善和建立数据备份恢复机制和残余信息保护措施，保证当用户数据发生异常时能够及时地进行恢复，保证当存储资源被重新分配给新用户时，提前做好可靠的数据擦除，防止原用户数据被非法恢复。服务提供商和企业提供不同的权限，对数据的安全提供保障。企业应该拥有完全的控制权限，对服务提供商限制权限。数据在网络传输到云中处理过程中需要得到保护，在传输过程中可以使用 SSL、VPN 等不同的传输方式，确保数据传输安全。

建立纵深防御机制，确保基础网络安全，建立集中统一的云计算安全服务中心。在云计算环境下，物理的安全边界逐步消失，云计算平台的用户只能依靠基于逻辑的划分来实现隔离，而不再是以往基于单个或者按照类型来进行划分，更不能只实施简单的流量汇聚或部署孤立的安全防护系统来保障整个平台的安全。因此，必须将安全服务的部署应用由基于各子系统的安全防护，转变为基于整个云计算架构网络的安全防护，提供集中统一的安全服务，从而适应这种逻辑隔离模型的要求。通过 VPN 和数据加密等技术，构建安全的逻辑边界。利用搭建好的技术安全通道，将提出安全服务需求的用户数据流，交付至安全服务中心分析处理，当服务完成后再按原有的转发路径返回至用户端，保障用户数据的网络传输安全。完善云计算平台的容灾备份机制，包括重要系统、数据的异地容灾备份。建立云计算系统的纵深安全防御机制，就是要覆盖整个云计算服务的后台、网络和前端，从而提高整个云

计算平台的安全性、可靠性,保障云计算服务的稳定性和连续性。

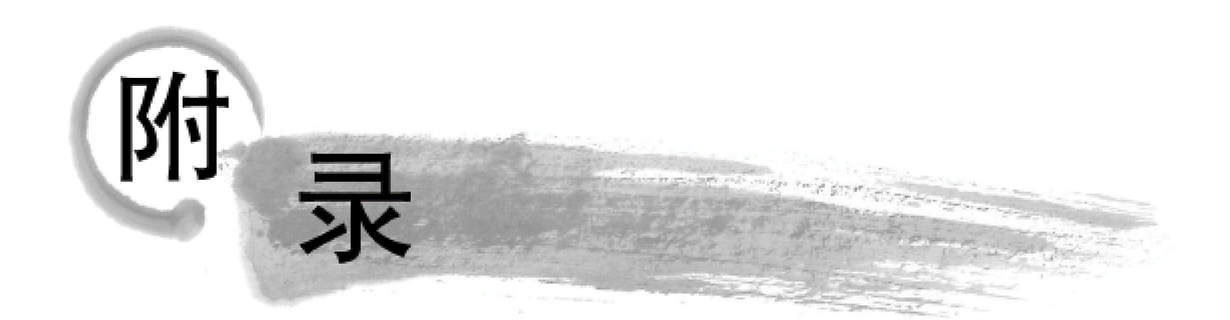
针对安全风险的挑战,对应对措施加以总结,如表11-1所示。

表11-1　云计算安全控制措施

安全性要求	其他用户	云服务商
数据访问的权限控制	权限控制程序	权限控制、合同规范
数据存储的私密性	存储隔离	存储加密、文件系统加密
数据运行时的私密性	虚拟机隔离、操作系统隔离	操作系统隔离
数据在网络上传输的私密性	传输层加密	传输层加密
数据的完整性	数据校验	数据校验
数据的持久可用性	数据备份、数据镜像	分布式存储
数据的访问速度	数据缓存	高速网络、CDN

思考题

1. 试归纳云计算的体系结构。
2. 详细解释云计算的特点。
3. 归纳云计算所面临的安全问题。
4. 查阅资料,试述云计算的风险评估流程。
5. 查阅资料,归纳云计算的安全措施。



信息安全管理与风险评估相关表格(参考示例)

如附表1所示为信息安全方针文件。

附表1　信息安全方针文件

<table>
<tr><td colspan="3">信息安全方针文件</td></tr>
<tr><td colspan="3">文档信息：</td></tr>
<tr><td colspan="3">编号：</td></tr>
<tr><td colspan="3">分类：(密级)</td></tr>
<tr><td>作者：</td><td>审核：</td><td>批准：</td></tr>
<tr><td colspan="3">版本及历史：</td></tr>
<tr><td>版本：</td><td>时间：</td><td>备注：</td></tr>
<tr><td colspan="3">修改历史：</td></tr>
<tr><td colspan="3">组织名称
日期</td></tr>
<tr><td colspan="3">1　目的
本文件是根据整体业务目标制定的信息安全活动的方针指导，公司管理者通过在整个组织中颁布和维护信息安全方针来表明对信息安全的支持和承诺。
信息安全管理体系方针指明了公司的信息安全目标和方向，并可以确保信息安全管理体系被充分理解和贯彻实施。
2　适用范围
本文件适用于信息安全管理体系涉及的所有人员和过程。
3　信息安全定义
信息安全是指保证信息的保密性、完整性、可用性，也可包括诸如真实性、可核查性、不可否认性和可靠性等属性。
信息安全是通过实施一组合适的控制措施而达到的，包括策略、过程、程序、组织结构以及软件和硬件功能。在需要时，需建立、实施、监视、评审和改进这些控制措施，以确保满足该组织的特定安全和业务目标。这个过程应与其他业务管理过程联合进行。
4　信息安全方针
信息安全可保护信息免受各种威胁的损害，以确保业务连续性、业务风险最小化，投资回报和商业机遇最大化。</td></tr>
</table>

续表

公司信息安全方针为：积极防御、安全管理、控制风险、保障安全。公司可根据实际需要，再制定其他重要领域的具体方针。

5 信息安全目标

公司的信息安全目标为满足已识别的信息安全要求，包括：

1）法律、法规和合同要求；

2）公司风险评估的结果。

公司信息安全的具体目标包括：

1）

2）

3）……

6 ISMS 范围

公司信息安全管理体系的范围覆盖如下业务：

1）内部办公系统；

2）财务系统；

3）……

其他说明。

7 安全管理机构

7.1 信息安全领导小组

信息安全领导小组是本公司信息安全管理工作的最高领导机构，承担信息安全活动在部门之间的协调。

7.2 信息安全推进小组

信息安全推进小组在信息安全领导小组的领导下，负责公司日常信息安全的管理与监督活动……

8 风险管理框架

……

9 重要原则和符合性要求

9.1 法律法规和合同要求的符合性

……

9.2 安全教育、培训和意识要求

……

9.3 违反信息安全方针的后果

……

……

10 评审

本文件按计划的时间间隔或当重大变化发生时进行信息安全方针评审，以确保其持续的适宜性、充分性和有效性。

公司每 12 个月评审一次本文件。在下列情况下，临时启动评审活动：

1）公司业务环境发生变化；

2）公司面临的威胁发生巨大的变化；

3）发生了重大的信息安全事故。

11 实施时间

……

12 相关文件

如附表 2 所示为适用性声明(A.5、A.6)。

附表 2 适用性声明(A.5、A.6)

条款		目标	控制措施	是否选择	涉及文件与记录或不选择的理由
A.5 安全方针					
A.5.1 信息安全方针					
A.5.1.1	信息安全方针文件	依据业务要求和相关法律法规提供管理指导并支持信息安全	信息安全方针文件应由管理者批准、发布并传达给所有员工和外部相关方	选择	《信息安全方针文件》
A.5.1.2	信息安全方针的评审		应按计划的时间间隔或当重大变化发生时进行信息安全方针评审,以确保它持续的适宜性、充分性和有效性	选择	《信息安全方针文件》、《管理评审程序》
A.6 信息安全组织					
A.6.1 内部组织					
A.6.1.1	信息安全的管理承诺	在组织内管理信息安全	管理者应通过清晰的说明、可证实的承诺、明确的信息安全职责分配及确认,来积极支持组织内的安全	选择	《信息安全方针文件》、《信息安全组织》
A.6.1.2	信息安全协调		信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调	选择	《信息安全方针文件》、《信息安全组织》
A.6.1.3	信息安全职责的分配		所有的信息安全职责应予以清晰地定义	选择	《信息安全方针文件》、《信息安全组织》
A.6.1.4	信息处理设施的授权过程		新信息处理设施应定义和实施一个管理授权过程	选择	《物理设备管理程序》
A.6.1.5	保密性协议		应识别并定期评审反映组织信息保护需要的保密性或不泄漏协议的要求	选择	《信息安全保密程序》
A.6.1.6	与政府部门的联系		应保持与政府相关部门的适当联系	选择	《政府、特定利益集团联系表》
A.6.1.7	与特定权益团体的联系		应保持与特定权益团体、其他安全专家组和专业协会的适当联系	选择	《政府、特定利益集团联系表》
A.6.1.8	信息安全的独立评审		组织管理信息安全的方法及其实施(例如信息安全的控制目标、控制措施、策略、过程和程序)应按计划的时间间隔进行独立评审,当安全实施发生重大变化时,也要进行独立评审	选择	《内部评审程序》、《管理评审程序》、《记录管理程序》、《文件管理程序》

续表

条款		目标	控 制 措 施	是否选择	涉及文件与记录或不选择的理由
A.6.2　外部各方					
A.6.2.1	与外部各方相关风险的识别	保持组织的被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全	应识别涉及外部各方业务过程中组织的信息和信息处理设施的风险,并在允许访问前实施适当的控制措施	选择	《信息安全保密程序》、《物理设备管理程序》、《控制访问管理程序》
A.6.2.2	处理与客户有关的安全问题		应在允许顾客访问组织信息或资产之前处理所有确定的安全要求	选择	《控制访问管理程序》
A.6.2.3	处理第三方协议中的安全问题		涉及访问、处理或管理组织的信息或信息处理设施以及与之通信的第三方协议,或在信息处理设施中增加产品或服务的第三方协议,应涵盖所有相关的安全要求	选择	《信息管理保密程序》、《控制访问管理程序》

如附表 3 所示为不符合报告。

附表 3　不符合报告

报告编号:

被审核部门:	审核时间:

不符合事实陈述:

……

以上事实不符合 XXX 要求。

不符合:　文件:

标准条款:

不符合类型:　□严重　□轻微

审核员:　部门负责人:

原因分析:

(1)

(2)

……

纠正措施计划:

(1)

(2)

(3)

……

纠正措施的预订完成时间:

部门负责人:　日期:

审核员:　日期:

信息安全管理经理:　日期:

续表

纠正措施完成情况： （1） （2） （3） …… 部门负责人：　　　　　　　　　　日期：
完成纠正措施的验证情况： （1） （2） （3） …… 审核员：　　　　　　　　　　日期：

如附表 4 所示为信息安全事件报告。

附表 4　信息安全事件报告

事件发生日期		相关事件的识别号（如果可能）	
事件号			
报告人信息			
姓名		电话	
组织		电子邮件	
地址			
信息安全事件描述			
事件描述	发生了什么		
	怎样发生的		
	为什么发生		
	受影响的组件		
	业务影响		
	任意已识别的脆弱点		
信息安全事件详细信息			
事件发生的日期和时间			
事件被发现的日期和时间			
事件被记录的日期和时间			
事件是否已经结束	是□否□		
（如果选择是）事件持续了多久（日/小时/分钟）			

如附表 5 所示为信息安全事故报告。

附表 5　信息安全事故报告

事故发生日期		相关事故的识别号（如果可能）	
事故号			
操作支持组成员信息			
姓名		电话	
地址		电子邮件	
信息安全事故描述			
事故描述	发生了什么		
	怎样发生的		
事故描述	为什么发生		
	受影响的组件		
	业务影响		
	任意已识别的脆弱点		
信息安全事故详细信息			
事故发生的日期和时间			
事故被发现的日期和时间			
事故被记录的日期和时间			
事故是否已经结束		是□否□	
（如果选择是）事故持续了多久(日/小时/分钟)			
（如果选择否）说明事故到目前为止持续了多久(日/小时/分钟)			
信息安全事故类型			
（选择一项,然后填写相关栏目）		实际发生的□未遂的□ 可疑的□	
（选择一项）蓄意的□		（表明所涉威胁类型）	
盗窃(TH)□		黑客攻击/逻辑渗透(HA)□	
欺诈(FR)□		滥用资源(MI)□	
破坏/物理损害(SA)□		其他(OD)□	
恶意代码(MC)□		具体说明:	
（选择一项）意外的□		（表明所涉威胁类型）	
硬件故障(HF)□		其他自然事件(NE)□	
软件故障(SF)□		通信故障(CF)□	
重要服务丧失(LE)□		火灾(FI)□	
人员短缺(SS)□		洪水(FL)□	
其他(OA)□		具体说明:	
（选择一项）错误□		（表明所涉威胁类型）	
操作错误(OE)□		用户错误(UE)□	
硬件维护错误(CHE)□		设计错误(DE)□	
软件维护错误(SE)□		其他(包括单纯错误)(OA)□	
		具体说明:	
未知的□(如果尚无法确定事故属于蓄意、意外还是错误造成的,选择本项,如果可能,用上述威胁类型缩写表明所涉威胁类型） 具体说明:			
受影响的资产			

续表

<table>
<tr><td colspan="3">（提供受事故影响或与事故有关的资产的描述，包括相关序号、许可证和版本号）
（如果有）</td></tr>
<tr><td>信息/数据</td><td colspan="2"></td></tr>
<tr><td>硬件</td><td colspan="2"></td></tr>
<tr><td>软件</td><td colspan="2"></td></tr>
<tr><td>通信设施</td><td colspan="2"></td></tr>
<tr><td>文档</td><td colspan="2"></td></tr>
<tr><td>事故对业务的负面影响</td><td colspan="2"></td></tr>
<tr><td>（用“1～5”在“数值”项中记录事故对所涉各业务造成负面影响的程度。如果了解实际成本，可填写到“成本”项中）</td><td>数值</td><td>成本</td></tr>
<tr><td>破坏保密性□（即未经授权泄漏）</td><td></td><td></td></tr>
<tr><td>破坏完整性□（即未经授权篡改）</td><td></td><td></td></tr>
<tr><td>破坏可用性□（即无法使用）</td><td></td><td></td></tr>
<tr><td>从事故中恢复的全部成本</td><td></td><td></td></tr>
<tr><td rowspan="2">（如果可能，填写事故恢复的实际总成本，用“1～10”填写“数值”项，用实际成本填写“成本”）</td><td>数值</td><td>成本</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="3">事故的解决</td></tr>
<tr><td>事故调查开始日期</td><td colspan="2"></td></tr>
<tr><td>事故调查员姓名</td><td colspan="2"></td></tr>
<tr><td>事故结束日期</td><td colspan="2"></td></tr>
<tr><td>影响结束日期</td><td colspan="2"></td></tr>
<tr><td>事故调查完成日期</td><td colspan="2"></td></tr>
<tr><td>调查报告的引用和位置</td><td colspan="2"></td></tr>
<tr><td>所涉人员/作恶者</td><td colspan="2"></td></tr>
<tr><td colspan="3">（选择一项）人员(PE)□合法建立的机构/部门(OI)□
机构的工作组(GR)□事故(AC)□
无作恶者(NP)□
如自然因素、设备故障、人为错误</td></tr>
<tr><td colspan="3">作恶者的动机描述</td></tr>
<tr><td colspan="3">（选择一项）犯罪/经济收益(CG)□消遣/黑客攻击(PH)□
政治/恐怖主义(PT)□报复(RE)□
其他(QM)□
具体说明：</td></tr>
<tr><td colspan="2">已采取的解决事故措施</td><td></td></tr>
</table>

如附表 6 所示为应急软硬件工具一览表。

附表 6　应急软硬件工具一览表

类别	序号	名　　称	单位	功能和用途
硬件	1	专用调查取证分析仪(不含软件)	台	专业的司法调查、取证、分析工具,可以在完全的保护模式下对 IDE、SATA、SCSI 等接口的磁盘进行镜像、分析等
	2	硬盘拷贝机	套	专用的硬盘复制工具,支持 IDE、SATA、SCSI 接口的硬盘复制、检测、对比等
	3	笔记本	台	2GB 内存、千兆网卡,安装有 Linux、Windows 2000、Windows 2003 Server 等
	4	3.5 英寸移动硬盘	块	
	5	3.5 英寸移动硬盘盒	个	
	6	5.25 英寸 IDE 硬盘	块	
	7	5.25 英寸 IDE 硬盘盒	个	
	8	2.5 英寸移动硬盘 IDE 接口卡	个	
	9	IDE 转 SCSI 桥	个	
	10	IDE 转 IEEE 1394 桥	个	
	11	IDE 转 USB 桥	个	
	12	USB 转串口桥	个	
	13	USB 转 PS2 桥	个	
	14	USB 键盘/鼠标	套	
	15	USB 2.0 转 RJ45 桥	个	
	16	USB 视频适配器	个	
	17	网络综合协议分析仪	台	
	18	10/100M 自适应 Hub	台	
	19	DVD/CD-RW 刻录机	台	
	20	DVD/CD-RW 光盘	盒	
	21	油性笔	支	
	22	数码相机	台	
	23	数码摄像机	台	
软件	24	专用调查取证分析仪配套软件		
	25	专用分析软件	套	专用的计算机取证工具包,具备快速的数据搜索、分析功能,具备口令恢复(包括 Office、PDF、Lotus 文档等)、注册表查看等功能
	26	Windows XP Home Edition	套	系统盘
	27	Windows XP Professional Edition	套	系统盘
	28	Windows Server 2003	套	系统盘
	29	Windows 7	套	系统盘
	30	Windows 8	套	系统盘
	31	Winternals ERD Commander 2005	套	Windows 光盘自启动工具。可以从光盘启动 Windows,查看 NT-FS 分区,修改 Windows 2000/XP/ Server 2003 开机口令,以及数据恢复、网络连接等功能

续表

类别	序号	名　　称	单位	功能和用途
软件	32	Linux 系统盘	套	系统盘
	33	Solaris 系统盘	套	系统盘
		BackTrack	套	基于 Slackware 和 SLAX 的自启动运行光盘，包含一套安全及计算机取证工具。通过融合 Auditor Security Linux 和 WHAX（先前的 Whoppix）创建而成
		KNOPPIX	套	Linux 下的光盘自启动工具，可以从光盘启动 Linux 系统
	34	Windows 主机数据初步收集工具包	套	常用工具套件，包含对 Windows 主机系统进行初步数据收集时常用的可信程序
	35	Linux 主机数据初步收集工具包	套	常用工具套件，包含对 Linux 主机系统进行初步数据收集时常用的可信程序
	36	Windows 主机数据深入收集工具包	套	常用工具套件，包含对 Windows 主机系统进行深入数据收集时常用的可信程序
	37	Linux 主机数据深入收集工具包	套	常用工具套件，包含对 Linux 主机系统进行深入数据收集时常用的可信程序
	38	Windows 主机数据分析工具包	套	常用工具套件，包含对 Windows 主机系统进行数据分析时常用的可信程序
	39	Linux 主机数据分析工具包	套	常用工具套件，包含对 Linux 主机系统进行数据分析时常用的可信程序
	40	网络数据收集工具包	套	常用工具套件，包含对常见网络设备进行初步数据收集时常用的可信程序
	41	网络数据分析工具包	套	常用工具套件，包含对常见网络设备进行数据分析时常用的可信程序

参 考 文 献

[1] 孙强，陈伟，王东红．信息安全管理全球最佳实务与实施指南．北京：清华大学出版社，2004.

[2] 范红，冯登国，吴亚非．信息安全风险评估方法与应用．北京：清华大学出版社，2006.

[3] 中国标准出版社第四编辑室．信息安全标准汇编 信息安全管理卷．北京：中国标准出版社，2008.

[4] 谢宗晓，郭立生．信息安全管理体系应用手册——ISO/IEC 27001 标准解读及应用模板．北京：中国标准出版社，2008.

[5] 范红．信息安全风险评估规范国家标准理解与实施．北京：中国标准出版社，2007.

[6] 吴亚非，李新友，禄凯．信息安全风险评估．北京：清华大学出版社，2007.

[7] 于军．信息安全管理的体系化管理——ISMS 在电子政务中的应用．北京：国防工业出版社，2008.

[8] 张红旗，王新昌，杨英杰等．信息安全管理．北京：人民邮电出版社，2007.

[9] 张泽虹，赵冬梅．信息安全管理与风险评估．北京：电子工业出版社，2010.

[10] 王春东，杨宏，赵俊阁．信息安全管理．武汉：武汉大学出版社，2008.

[11] 吴晓平，付钰．信息系统安全风险评估理论与方法．北京：科学出版社，2011.

[12] 刘换，赵刚．人工智能在信息安全风险评估中的应用．北京信息科技大学学报（自然科学版），2012，27(4)：59-63.

[13] 李艳杰．GB/T 22080—2008《信息安全管理体系 要求》解析．中国标准导报，2012，10：6-9.

[14] 许玉娜，罗锋盈，陈星．SP 800-39：2011 信息安全风险管理研究．信息技术与标准化，2012，4：41-44.

[15] 胡灵娟．大型数据中心 ISO 27001 信息安全管理体系贯标认证实践．中国金融电脑，2012，5：32-37.

[16] 赵战生．完善信息安全管理标准 落实信息安全等级保护制度．信息网络安全，2008，1：15-18.

[17] 陈清明，张俊彦．信息安全风险评估工具及其应用分析．信息安全与通信保密，2010，1：93-95.

[18] 王亚东，吕丽萍，汤永利等．信息安全管理体系与等级保护的关系研究．北京电子科技学院学报，2012，20(2)：26-31.

[19] 赵刚，刘换．基于多层次模糊综合评判及熵权理论的实用风险评估．清华大学学报（自然科学版），2012，52(10)：1382-1387.

[20] 马遥，黄俊强．信息安全管理体系与等级保护管理要求．信息技术，2012，6：140-142.

[21] 周佑源，张晓梅．信息安全管理在等级保护实施过程中的要点分析．信息安全与通信保密，2009，9：66-68.

[22] 黄成哲．信息安全风险评估工具综述．黑龙江工程学院学报，2006，20(1)：45-48.

[23] 蔡盈芳．基于云计算的信息系统安全风险评估模型．中国管理信息化，2010，13(12)：75-77.

[24] 汪兆成．基于云计算模式的信息安全风险评估研究．信息网络安全，2011，9：56-59.

[25] 薄明霞，陈军，王渭清等．浅谈云计算的安全隐患及防护策略．信息安全与技术，2011，9：62-64.

[26] 刘波．云计算的安全风险评估及其应对措施探讨．移动通信，2011，9：34-37.

[27] 董建锋，裴立军，王兰英．云计算环境下信息安全分级防护研究．信息网络安全，2011，6：38-40.